AYRIK MATEMATİKTE İLERİ KONULAR(DERS NOTLARI)

1 Mantık, bağıntı, fonksiyonlar, Küme Teorisi ve Temel K.

1.1 Önerme Mantığı ve İspatlar

Mantık önermelerin doğruluğunu kanıtlamak için kullanılır. Önermenin ne olduğu ile ilgilenmek yerine bazı kurallar koyar ve böylece önermenin genel formunun geçerli olup olmadığını yargılar. Mantığın bize sağladığı kurallar, belirtilen aşamalardan çıkan sonucun tutarlı olup olmadığını veya sonucun doğruluğunun ispatlanması aşamasındaki basamaklarda hatalı bir kısmın bulunup bulunmadığını değerlendirmemizi sağlar.

1.1.1 Önermeler ve Doğruluk Tabloları

Önerme, doğru veya yanlış değerinden sadece ve sadece birini alabilen ifadedir. Fakat aynı anda iki değeri birden alamaz. Örneğin aşağıdaki ifadeler birer önermedir.

1. Bu gül beyazdır.
2. Üçgenin dörtkenarı vardır.
3. 3 + 2 = 6.
4. 6 < 24
5. Yarın benim doğum günümdür.

Aynı önermenin nerede, ne zaman ve kim tarafından söylendiğine bağlı olarak bazen doğru bazen yanlış olabileceğine dikkat ediniz. Yarın doğum günü olan biri için 5. önerme doğru iken, başka biri tarafından ifade edildiğinde yanlış olacaktır. Hatta bugün herhangi biri için doğru olan bir önerme başka bir gün için yanlış olabilir.

Ünlemler, sorular ve istekler doğru veya yanlış diye ifade edilemediklerinden birer önerme değildirler. Bu nedenle aşağıdakiler önerme değildir.

6. Çimlerden uzak durun.
7. Çok yaşa kraliçe!
8. Jane'in partisine gittin mi?
9. Öyle söyleme.

Bir önermenin doğruluğu (T) veya yanlışlığı (F) önermenin **doğruluk değeri** şeklinde adlandırılır. 4. önerme doğru (T) doğruluk değerini taşırken, 2 ve 3. önermeler yanlış (F) doğruluk değerini taşır. 1 ve 5 numaralı önermenin doğruluk değerleri ifade edildikleri duruma bağlıdır.

Geleneksel olarak önermeler p,q,r… harfleri kullanılarak sembolize edilirler. Örneğin p: Manchester İskoçya'dadır, q: Dinozorlar hala yaşamaktadır.

1.1.2 Mantıksal Bağlılıklar ve Doğruluk Tabloları

Bundan önceki konudaki 1-5 numaralı ifadeler basit birer ifade oluşturduklarından **basit önerme**lerdir. Bu bölümde basit önermelerin nasıl bağlanarak **bileşik önerme**ler şeklinde adlandırılan daha karışık önermeler oluşturulacağı anlatılacaktır. Önerme çiftlerini bağlamaya yarayan araçlara mantıksal bağlayıcılar denir ve herhangi bir bileşik önermenin doğruluk değeri tamamen (a) kendisini oluşturan basit önermelerin doğruluk değerleri (b) bunları bağlayan özel bağlayıcı veya bağlayıcılar tarafından belirlenir.

En çok kullanılan bağlaçlara geçmeden önce, basit bir önerme üzerinde gerçekleştirilebilen bir işleme bakalım. Bu işleme **tersini alma** denir ve önermenin doğruluk değerini tersine çevirme etkisi yapar. Tersini alma sonucunda önerme eğer doğru ise yanlış, yanlış ise doğru değerini alır. Bu işlemi bir tablo ile özetleyebiliriz. Eğer p bir önermeyi sembolize ediyorsa, $\overline{p}$ (~p,-p veya $\neg$p) p' nin tersini temsil eder. Aşağıdaki tablo p ve $\overline{p}$ 'nün doğruluk değerleri arasındaki ilişkiyi gösterir.

p	$\overline{p}$
T	F
F	T

Soldaki sütun p için tüm olası doğruluk değerlerini verirken sağ sütun p' nin tersi $\overline{p}$ için karşılık gelen doğruluk değerlerini verir. Bu şekilde, önermelerin doğruluk değerlerini özetleyen tabloya **doğruluk tablosu** denir.

Bir önermenin tersini ifade etmenin çeşitli yolları vardır. "Bütün köpekler vahşidir" önermesini düşünürsek, bu önermenin tersi şunlar olabilir:

Bütün köpeklerin vahşi olması söz konusu değildir.
Köpeklerin hepsi vahşi değildir.
Bazı köpekler vahşi değildir.

Dikkate edilirse "Hiçbir köpek vahşi değildir" önermesi "Bütün köpekler vahşidir" önermesinin tersi değildir. Tersini alma işleminde, ilk ifadenin doğru olduğu her durumda ikinci ifade yanlış olmalı ya da tam tersi olmalıdır. "Bütün köpekler vahşidir" önermesi sadece bir köpek bile vahşi olduğunda yanlıştır ancak "Hiçbir köpek vahşi değildir" önermesi bu durumda doğru değildir.

Mantıksal bağlayıcılar önerme çiftlerini bağlamaya yararlar. Burada çok kullanılan beş mantıksal bağlayıcıdan bahsedilecektir: kesişim, dahili birleşim, harici birleşim, koşullu önerme ve iki yönlü koşullu önerme.

1.1.3 Kesişim (Conjunction)

İki basit önerme aralarına 've' kelimesi koyarak bağlanabilir. Bunun sonucunda oluşan bileşke önermeye iki basit önerme bileşeninin kesişimi denir. Eğer p ve q iki basit önerme ise $p \wedge q$ (veya p.q) p ve q 'nun birleşimini temsil eder.

p: Güneş Parlıyor.
q: Köpekler havlar.
$p \wedge q$: Güneş parlıyor ve köpekler havlar.

Alttaki doğruluk tablosu p ve q 'nun tüm olası doğruluk değerleri için $p \wedge q$ 'nun doğruluk değerlerini gösterir.

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Yukarıdaki tablodan da görülebildiği gibi $p \wedge q$ sadece p ve q 'nun her ikisinin de doğru olduğu zaman doğrudur.

1.1.4 Birleşim (Disjunction)

Veya kelimesi iki basit önermeyi birleştirmek için kullanılabilir. Oluşan bileşke önerme iki basit önermenin birleşimi olarak adlandırılır. Mantıkta iki çeşit birleşim vardır: dahili ve harici. Gerçek hayatta kullandığımız veya kelimesi bazen kafa karıştırıcı olabilir.

p ve q birer önerme ise p v q, p ve q 'nun dahili birleşimini temsil eder. Bu bileşke önerme bileşenlerinden herhangi birisi veya her ikisinin doğru olması durumunda doğru aksi halde yanlıştır. $p \vee q$ için doğruluk tablosu aşağıdadır.

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

p ve q' nun harici birleşimi ise $p \veebar q$ şeklinde gösterilir. Bu bileşke önerme sadece bir bileşenin doğru olması durumunda doğrudur. $p \veebar q$ 'nun doğruluk tablosu aşağıdaki gibidir:

p	q	$p \veebar q$
T	T	F
T	F	T
F	T	T
F	F	F

İki basit önerme "veya" kullanılarak bağlanırken hangi tip birleşimin kullanılacağı cümlenin genel durumundan anlaşılır. Örneğin, 'Yarın yüzmeye gideceğim veya golf oynayacağım' cümlesi iki işin birden yapılmayacağı anlamı taşıdığından harici tiptedir. Diğer taraftan, 'Adaylar 25 yaşın üzerinde veya en az 3 yıllık tecrübeye sahip olmalıdır' cümlesinde iki şarttan birini sağlayan adaylar dikkate alınacakmış izlenimi verdiğinden dahili birleşimidir.

1.1.5 Koşullu Önermeler

Koşullu önerme bağlayıcısı → işareti ile sembolize edilir. Koşullu önermenin normal dildeki karşılığı örnekte de görüleceği gibi 'Eğer …' dır.

p: Kahvaltı yaparım.
q: Öğlen yemeği yemem.
$p \rightarrow q$: Eğer kahvaltı yaparsam, öğlen yemeği yemem.

Yukarıdaki örnekteki $p \rightarrow q$ için diğer alternatifler:

Sadece eğer öğlen yemeği yemezsem kahvaltı yaparım.
Kahvaltı yapmam öğlen yemeği yemeyeceğim anlamına gelir.
Ne zaman kahvaltı yapsam öğlen yemeği yemem.

Aşağıdaki tablo $p \rightarrow q$' nun doğruluk tablosudur.

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Dikkat edilirse ‘p ise q’ önermesi sadece p’ nin doğru q’ nun yanlış olması durumunda yanlıştır.(örneğin doğru bir ifade yanlış bir ifade anlamına gelemez.) Eğer p yanlış ise bileşke önerme q nun doğruluk değeri ne olursa olsun doğrudur. Şu önermeye bakalım: ‘Eğer derslerimi geçersem çok sevineceğim’. Bu ifade eğer sınavlarımı geçemezsem ne yapacağım hakkında hiçbir şey söylemiyor. Belki sevinirim, belki sevinmem ama hiçbir durumda söylenen ifade yanlış değildir. Önermenin yanlış olabileceği tek durum sınavlarımı geçip sevinmediğim durumdur.

Koşullu önermelerde, p önermesi önceki ve q önermesi sonraki olarak adlandırılır. p önermesi q için **yeterli** şart, q ise p için **gerekli** şarttır.

1.1.6 Çift Yönlü Koşullu Önermeler

Çift yönlü koşullu bağlayıcı ↔ ile gösterilir ve ‘sadece ve sadece …. ise …….’ şeklinde ifade edilir. Önceki örneğe tekrar dönersek:

p: Kahvaltı yaparım.
q: Öğlen yemeği yemem.
p ↔ q : Sadece ve sadece öğlen yemeği yemezsem kahvaltı yaparım.(alternatif olarak sadece ve sadece kahvaltı yaparsam öğlen yemeği yemem.)

p ↔ q ‘nin doğruluk tablosu şu şekildedir:

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Dikkat edilirse p ↔ q nun doğru olabilmesi için p ve q nun her ikisinin de aynı doğruluk değerine sahip olması gerekir.

Örnek 1.1: p, ‘Bugün Pazartesi’ ve q ‘İstanbul’a gideceğim’ önermeleri olsun. Buna göre aşağıdaki önermeleri sembollerle ifade ediniz.

(i) Eğer bugün Pazartesi ise İstanbul’a gitmeyeceğim.
(ii) Bugün Pazartesi veya İstanbul’a gideceğim fakat ikisi birden değil.
(iii) Bugün İstanbul’a gideceğim ve bugün Pazartesi değil.
(iv) Sadece ve sadece bugün Pazartesi değilse İstanbul’a gideceğim.

Çözüm 1.1:

(i) $p \rightarrow \overline{q}$
(ii) $p \veebar q$
(iii) $q \wedge \overline{p}$
(iv) $\overline{p} \leftrightarrow q$.

Örnek 1.2: Aşağıdaki bileşik önermeler için doğruluk tabloları oluşturunuz.

(i) $\overline{p} \vee q$

(ii) $\overline{p} \wedge \overline{q}$

(iii) $\overline{q} \rightarrow$p

(iv) $\overline{p} \leftrightarrow \overline{q}$

Çözüm 1.2:

(i)

p	q	$\overline{p}$	$\overline{p} \vee q$
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

(ii)

p	q	$\overline{p}$	$\overline{q}$	$\overline{p} \wedge \overline{q}$
T	T	F	F	F
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

(iii)

p	q	$\overline{q}$	$\overline{q} \rightarrow$p
T	T	F	T
T	F	T	T
F	T	F	T
F	F	T	F

(iv)

p	q	$\overline{p}$	$\overline{q}$	$\overline{p} \leftrightarrow$
T	T	F	F	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

1.1.7 Tutolojiler ve Çelişkiler

Bileşenlerinin doğruluk değeri ne olursa olsun her zaman doğru olan birçok bileşik önerme mevcuttur. Benzer şekilde bileşenlerinden bağımsız olarak her zaman yanlış olanlar da vardır. Her iki durumda da bu özellik bileşke önermenin yapısının sonucudur.

Tutoloji, basit bileşenlerinin doğruluk değeri ne olursa olsun doğru olan bileşke önermedir. Örnek : insanlar erkektir veya kadındır önermesi her zaman doğrudur. O nedenle bu önerme bir tutolojidir.

Çelişki ise, basit bileşenlerinin doğruluk değeri ne olursa olsun yanlış olan bileşke önermedir.

Tutoloji *t* ile, çelişki ise *f* ile gösterilir.

Örnek 1.3 : $p \vee \overline{p}$‘nin tutoloji olduğunu gösteriniz.

Çözüm1.3 : Eğer $p \vee \overline{p}$ 'in doğruluk tablosunu yaparsak:

p	$\overline{p}$	$p \vee \overline{p}$
T	F	T
F	T	T

Dikkat edilirse $p \vee \overline{p}$ her zaman doğru değerini verir (p yerine hangi önerme konulursa konulsun) ve bu sebeple tutolojidir.

Örnek 1.4 : $(p \wedge q) \vee (\overline{p \wedge q})$ 'nin tutoloji olduğunu gösteriniz.

Çözüm 1.4 : Verilen önermenin doğruluk tablosu aşağıdaki gibidir:

p	q	$p \wedge q$	$\overline{p \wedge q}$	$(p \wedge q) \vee (\overline{p \wedge q})$
T	T	T	F	T
T	F	F	T	T
F	T	F	T	T
F	F	F	T	T

Doğruluk tablosunun en son sütunu sadece T doğruluk değerini gösterir ve bu nedenle $(p \wedge q) \vee (\overline{p \wedge q})$ ifadesi bir tutolojidir.

Son örnekte, ilk örnekten elde ettiğimiz 'herhangi bir önermenin tersinin dahili birleşimi bir tutolojidir' sonucunu kullanabilirdik. İkinci örnekte elimizde $p \wedge q$ önermesi ve tersi $\overline{p \wedge q}$ var. Bu nedenle önceki sonuca göre $(p \wedge q) \vee (\overline{p \wedge q})$ bir tutolojidir. $(p \wedge q) \vee (\overline{p \wedge q})$ önermesi, $p \vee \overline{p}$ önermesinin **yedek örneği**dir denir. Açıkça görülüyor ki, bir tutolojinin yedek örneği kendi başına bir tutolojidir ve dolayısıyla bir önermenin tutoloji olduğunu göstermenin bir yolu da bu önermenin tutoloji olduğu bilinen başka bir önermenin yedek örneği olduğunu göstermektir. Tıpkı tutolojilerde olduğu gibi bir çelişkinin de yedek örneği bir çelişkidir.

1.1.8 Mantıksal Eşdeğerlik ve Mantıksal Anlam

İki önerme, kendilerini oluşturan bileşenlerinin tüm doğruluk değeri kümesi için aynı doğruluk değerine sahipse bu iki önerme **mantıksal eşdeğer**dir denir. P ve Q iki bileşik önerme olsun, P ve Q mantıksal eşdeğerse P ≡ Q şeklinde gösterilir.Tutolojiler ve çelişkilerde olduğu gibi mantıksal eşdeğerlilik de P ve Q' nun yapılarının sonucudur.

Örnek 1.5 : $\overline{p} \vee \overline{q}$ ve $\overline{p \wedge q}$' nun mantıksal eşdeğer olduğunu gösteriniz.

Çözüm 1.5 : $\overline{p} \vee \overline{q}$ ve $\overline{p \wedge q}$ için doğruluk tablosunu çizelim.

p	q	$\overline{p}$	$\overline{q}$	$\overline{p} \vee \overline{q}$	$p \wedge q$	$\overline{p \wedge q}$
T	T	F	F	F	T	F
T	F	F	T	T	F	T
F	T	T	F	T	F	T
F	F	T	T	T	F	T

$\overline{p} \vee \overline{q}$ ve $\overline{p \wedge q}$ için hesaplanan sütunlardaki doğruluk değerleri karşılaştırılırsa aynı olduklarını

görülür. Bu nedenle bu iki önerme mantıksal eşdeğerdir denilebilir.

Eğer iki bileşke önerme mantıksal eşdeğerse, bu iki önermenin çift yönlü koşullu bağlayıcı ile bağlanmasıyla oluşan önerme bir tutoloji olmalıdır.($P \equiv Q$ ise $P \leftrightarrow Q$ tutoloji olmalı) Bunun nedeni, iki mantıksal eşdeğer önermenin ikisi de aynı anda ya doğrudur ya yanlıştır. Her iki durumda da çift yönlü koşullu önerme doğrudur. Bu durumun tersi de yani $P \leftrightarrow Q$ bir tutoloji ise $P \equiv Q$. Bunun nedeni şu gerçeğe dayanır: Çift yönlü koşullu önerme $P \leftrightarrow Q$ sadece P ve Q' nun her ikisinin de aynı doğruluk değerine sahip olduğu zaman doğrudur.

İki önerme arasında oluşabilecek bir diğer yapıya-bağımlı ilişki de mantıksal anlamdır. Eğer bir P önermesi her doğru olduğunda Q önermesi de doğru oluyorsa, P önermesi mantıksal olarak Q önermesi anlamına gelir. Ancak bunun tersi doğru değildir yani Q, P yanlış olduğunda da doğru olabilir. Mantıksal anlam $\vdash$ ile sembolize edilir. $P \vdash Q$, P mantıksal olarak Q anlamına gelir demektir.

Örnek 1.6: $q \vdash (p \vee q)$ olduğunu gösteriniz.

Çözüm 1.6: q'nun her doğru olduğu anda $(p \vee q)$ nun da doğru olduğunu göstermek gerekir. Doğruluk tablosunu yaparsak:

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

q'nun doğru olduğu her durumda (1 ve 3. satırlar) $p \vee q$ da doğrudur. $p \vee q$, q yanlış olduğunda da doğrudur (2. satır) fakat bunun q, $p \vee q$ ile mantıksal anlamdır ifadesinin sağlanmasıyla bir alakası yoktur.

'$P \vdash Q$' ile '$P \rightarrow Q$ bir tutolojidir' ifadeleri benzer ifadelerdir. $P \vdash Q$ ise P doğru iken Q hiçbir durumda yanlış değildir. Bu da sadece $P \rightarrow Q$' nun yanlış olduğu durumda mümkün olduğundan $P \rightarrow Q$ bir tutoloji olmalıdır.

1.1.9 Önermeler Cebri

Aşağıdaki liste bir önceki konudaki teknikler kullanılarak ispatlanabilecek mantıksal eşitlikleri içerir. Bu kurallar p, q ve r gibi basit önermeler ve bunların yerine konabilecek yedek örneklerin tamamı için geçerlidir.

Aynılık (Tek Kuvvet) Özelliği(idempotence)

$p \wedge p \equiv p$

$p \vee p \equiv p.$

Değişme Özelliği(Commutativity)

$p \wedge q \equiv q \wedge p$

$p \vee q \equiv q \vee p$

$p \veebar q \equiv q \veebar p$

$p \leftrightarrow q \equiv q \leftrightarrow p.$

Birleşme Özelliği(Associativity)

$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$

$(p \vee q) \vee r \equiv p \vee (q \vee r)$

$(p \veebar q) \veebar r \equiv p \veebar (q \veebar r)$

$(p \leftrightarrow q) \leftrightarrow r \equiv p \leftrightarrow (q \leftrightarrow r)$.

Yutan Eleman(absorbtion)

$p \wedge (p \vee q) \equiv p$

$p \vee (p \wedge q) \equiv p$.

Dağılma Özelliği(Distributivity)

$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

Çift ters Özelliği(Double negation), involution

$\overline{\overline{p}} \equiv p$.

De Morgan Kuralları

$\overline{p \vee q} \equiv \overline{p} \wedge \overline{q}$

$\overline{p \wedge q} \equiv \overline{p} \wedge \overline{q}$.

Özdeşlik Özelliği(identity)

$p \vee f \equiv p$

$p \wedge t \equiv p$

$p \vee t \equiv t$

$p \wedge f \equiv f$.

Tamamlama Özelliği(Complement)

$p \vee \overline{p} \equiv t$

$p \wedge \overline{p} \equiv f$

$\overline{f} \equiv t$

$\overline{t} \equiv f$

1.1.10 Eşlik Kuralı (Duality Principle)

Sadece $\vee$ ve $\wedge$ bağlayıcılarını içeren herhangi bir P önermesi verilmiş ise, bu önermenin eşi $\vee$ yerine $\wedge$, $\wedge$ yerine $\vee$, t yerine f ve f yerine de t koyarak elde edilir. Örneğin, $(p \wedge q) \vee \overline{p}$ ' nin eşi $(p \vee q) \wedge \overline{p}$ olmalıdır.

Dikkat edilirse kesişim ve dahili birleşim dışındaki bağlayıcılarla bağlanmış bileşik önermelerin eşinin nasıl elde edildiğinden bahsedilmedi. Bunun önemi yoktur çünkü diğer bağlayıcılara sahip önermelerin hepsi sadece tersini alma ve kesişim bağlayıcılarını içeren mantıksal eşdeğer formunda yazılabilir. Eşlik kuralına göre eğer iki önerme mantıksal eşdeğerse, eşleri de

mantıksal eşdeğerdir.

1.1.11 Yerine Koyma Kuralı

Diyelim ki, elimizde mantıksal eşdeğer P_1 ve P_2 önermeleri ile P_1 'i içeren Q bileşik önermesi var. Yerine koyma kuralına göre P_1 yerine P_2 koyarsak sonuçta oluşan önerme Q ile mantıksal eşdeğerdir. Bu sebeple mantıksal eşdeğer önermeleri birbirinin yerine koymak sonuçta oluşan önermenin doğruluk değerini değiştirmez. Bunun ispatı şu şekilde yapılabilir: Doğruluk tablosunda P_1 sütunu yerine P_2 sütununu koyarsak sonuç değişmez zira P_1 ve P_2 'nin doğruluk tabloları aynıdır.

Yerine koyma kuralı ve önermeler cebri kuralları doğruluk tabloları çizmeden önermeler arasında mantıksal eşitlikler kurabilmemizi sağlar.

Örnek 1.7: $(\overline{p} \wedge q) \vee \left(\overline{p \vee q}\right) \equiv \overline{p}$ olduğunu ispatlayınız.

Çözüm 1.7: $(\overline{p} \wedge q) \vee \left(\overline{p \vee q}\right) \equiv (\overline{p} \wedge q) \vee (\overline{p} \wedge \overline{q})$ (De Morgan Kuralı)

$\equiv \overline{p} \wedge \left(q \vee \overline{q}\right)$ (Dağılma özelliği)

$\equiv \overline{p} \wedge t$

$\equiv \overline{p}$

1.1.12 Koşullu önermeler ile ilgili diğer özellikler

Verilen $p \rightarrow q$ koşullu önermesi için;

a) $p \rightarrow q$ 'nün karşıtı(converse) $q \rightarrow p$

b) $p \rightarrow q$ 'nün tersi(inverse) $\overline{p} \rightarrow \overline{q}$

a) $p \rightarrow q$ 'nün ters pozitifi(contrapositive) $\overline{q} \rightarrow \overline{p}$

Doğruluk Tablosu

p	q	$p \rightarrow q$	$q \rightarrow p$	$\overline{p} \rightarrow \overline{q}$	$\overline{q} \rightarrow \overline{p}$
T	T	T	T	T	T
T	F	F	T	T	F
F	T	T	F	F	T
F	F	T	T	T	T

Tablodan $p \rightarrow q$ 'nün ters pozitifi olan, $\overline{q} \rightarrow \overline{p}$ 'nin mantıksal eşdeğer oldukları görülmektedir.

$$p \rightarrow q \equiv \overline{q} \rightarrow \overline{p}$$

Koşullu önermenin karşıtı veya tersi kendisi ile mantıksal eşdeğer değildir. Hâlbuki karşıt ve zıttı birbiriyle mantıksal eşdeğerdir.

Örnek: **p** : bu gün salı **q**: bu gün bir sınavım var

$p \rightarrow q$: eğer bugün salı ise bugün bir sınavım var

a) $p \rightarrow q$ 'nün karşıtı(converse) $q \rightarrow p$: Eğer bugün sınavım var ise bugün salı.

b) $p \rightarrow q$ 'nün tersi(inverse) $\overline{p} \rightarrow \overline{q}$: Eğer bu gün salı değil ise bugün sınavım yok

a) $p \rightarrow q$ ‘nün ters pozitifi(contrapositive) $\overline{q} \rightarrow \overline{p}$: Eğer bugün sınavım yok ise bugün salı değil.

Tez(Argument): birbirini oluşturan önemeleri dayanak olarak alan önemeler kümesine denir ve sonunda bir sonuca ulaşır. Dayanak noktalarındaki önermeler bağlaç ile birbirine bağlanırlar ve sonunda mantıksal bir sonuca ulaşırlar. Aksi halde tez geçersizdir.

Eğer dayanak noktasındaki önermeler P_1, P_2, …, P_n ve sonucu Q ise tez,

Eğer ($P_1 \wedge P_2 \wedge \ldots \wedge P_n$) ├ Q) veya ($P_1 \wedge P_2 \wedge \ldots \wedge P_n \rightarrow Q$) bir tutolojidir. P_1, P_2, …, P_n doğru olduğunda , Q doğru olmalıdır.

1.1.13 Yüklem mantığı(Predicate Logic)

Yüklem, bir veya birkaç nesnenin veya bireylerin özelliklerini açıklar.

…. kırmızı,

….. nın uzun dişleri var

……Başı üzerinde durmaktan hoşlanır . gibi.

Yüklemi ifade etmek için büyük harf ile semboller kullanırız.

M: kırmızıdır

B: uzun dişleri var

G: başının üzerinde durmaktan hoşlanır

Küçük harf semboller ise bireyleri ifade etmekte kullanılır.

a : bu gül

b: Ahmet

Basit önerme aşağıdaki gibi ifade edilebilir.

M(a) : Bu gül kırmzıdır

M(b) :Ahmet kırmızıdır

G(b) : Ahmet başı üzerinde durmaktan hoşlanır.

Eğer M , kırmızıdır yüklemi olarak ifade edilirse M ‘yi M(x) olarak ifade ederiz ve “x kırmızıdır” anlamına gelir. Burada x değişkeni, herhangi bir nesne veya birey adı ile yer değiştirilebilir. Bu nedenle M(x) önermesel fonksiyon olarak adlandırılır. Önermesel fonksiyonun tersi ,

Eğer M(x) : “x kırmızıdır” ise $\overline{M(x)}$: “x kırmızı değildir” anlamına gelir.

Evrensel Niteleyici :”Bütün sıçanlar gridir” önermesini düşünelim. Bunun ilk yolu bütün sıçanlar için ; eğer x bir sıçan ise x gridir . önermesi ifade edilebilir. Bu bize yeni bir gösterim tanımlamayı getirir.

R(x) : x bir sıçandır , G(x) : x gridir. Her x için ‘i $\forall$x olarak ifade edip

($\forall$x)[R(x) $\rightarrow$G(x)] şeklinde yazılır. Burada $\forall$ evrensel niteleyici olarak adlandırılır.

Varlık Niteleyici :Eğer aynı önermede “En az bir adet x” vardır’ı $\exists$x şeklinde ifade ederek, “Bazı sıçanlar gridir” önermesini; vardır şeklinde yazarız.

($\exists$x)[R(x) $\rightarrow$G(x)] olarak yazabiliriz burada $\exists$ ye varlık niteleyici denir ve en az bir x vardır veya bazı x’ler için şeklinde söylenir.

Yüklem mantığında Düşünceler

Yüklem mantığında bir tezin geçerliliği sağlanır. Bütün yüklemler doğruluğunun sağlandığı durumda sonuçta doğrudur. Aşağıdaki dört kural yüklem mantığında geçerlidir.

1. Evrensel tanım : Eğer önerme $(\forall x)F(x)$ doğru ise F(a) 'da evrendeki her a için doğrudur.

2. Evrensel Genelleştirme: Eğer önerme F(a), evrendeki her a için doğru ise $(\forall x)F(x)$ 'da doğrudur.

3. Varlık tanımı : Eğer önerme $(\exists x)F(x)$ doğru ise, evrende, F(a)'yı doğru yapan bir a vardır.

4. Varlık genelleştirmesi : Eğer önerme evrendeki bazı a'lar için F(a) doğru oluyorsa' $(\exists x)F(x)$ doğrudur.

Örnek 1.8.: Yeşil gözlü olan herkese güvenilmez. Ali'nin yeşil gözleri var. Öyleyse Ali'ye güvenilmez. Tezinin geçerliliğini gösterelim.

Eğer G(x) : x'in yeşil gözleri var ve T(x) : x güvenilir ve a , ali'yi gösterirse;

$(\forall x)[G(x) \rightarrow \overline{T(x)}]$ ve $G(a) \rightarrow \overline{T(a)}$ şeklindedir.

1.2 Matematiksel İspat

Matematiksel ispatın popüler görünümü genellikle sembollerle yazılan birtakım adımların ard arda sıralanması şeklindedir. Her bir adım mantıksal olarak ispatın bir önceki adımını takip eder ve son satır ispatlanacak ifadedir. Bu imaja bağlı olarak ortak kanı, ispatın matematiksel doğruluğun mutlak ve sıkı bir testi olmasıdır. Fakat sürpriz bir biçimde, kendi aralarında ortak bir kanı olmamasına rağmen, bu görüş çoğu profesyonel matematikçinin görüşü değildir. Çoğu ispatın sosyolojik boyutunun olduğu görüşünü savunur ve ispatı, fikirlerin açıklanması ve iletimi için bir şart olarak kabul eder.

Aslında her iki görüş de doğrudur. İspat kelimesi geniş bir yelpazeyi kapsar. Bu yelpazenin bir ucunda birinci bölümdeki mantıksal işaretlerle ifade edilen çok resmi ispatlar bulunur. Her bir adım bir önceki adımı mantık kuralları çerçevesinde takip eder. Aslında, ispat yapmak için sadece semboller kullanmak mümkündür fakat bu tabi ki takip etmesi zor bir olaydır. Daha az resmi ispatlar ise kelimelerin, sembollerin ve diyagramların karışımıyla gerçekleştirilir. Matematik ile ilgili kitaplardaki ispatlar genellikle az resmi ispatlardır.

Matematikte onay verilmeyen bir şey varsa o da gözlemlere dayanarak sonuca gitmektir. Öte yandan, birçok kez bir çift sayının karesini aldığımızda sonucun bir çift sayı olduğunu gözlememize rağmen bu çift sayıların karesinin çift sayı olduğunu kanıtlamaz. Ancak bu buna inancımızı kuvvetlendirir ve bu gözleme geçerli bir kanıt aramaya teşvik eder. Gözlemlere dayanarak çeşitli gerçekler hakkında yargılarda bulunmaya tümevarım denir. Mantıksal çıkarımlarla sonuca varılan yargıya ise tümdengelim denir.

1.2.1 Aksiyomlar ve Aksiyom Sistemleri

Matematiksel bir teori, örneğin küme teorisi, sayı teorisi veya grup teorisi değişik bileşenler içerir. Bunların en önemlileri:

1. Tanımlanmamış terimler.
2. Aksiyomlar.
3. Tanımlar.
4. Teoremler.
5. İspatlar.

3, 4 ve 5. maddelerde sıralananlar hakkında herkes bilgi sahibi olabilir. Matematikte

tanımlanmamış terimlere ihtiyaç duymamız sürpriz gelebilir fakat biraz düşünülürse bunun gerekliliği anlaşılabilir.

Diyelim ki, küme teorisi üzerine eksiksiz bir çalışma yapmak istiyoruz. Açıktır ki başlangıç noktası kümenin ne olduğunu anlatmaktır: Tanım 1: Küme …..- Yani? Problem şu ki, kümeyi tarif etmek için başka bir terime ihtiyacımız var (örneğin topluluk) ancak bu sefer de diğer terim tanımlanmamış durumdadır. Diğer terimi tanımlayabilmek için yine başka bir tanımlanmamış terime ihtiyacımız var ve bu böyle devam eder. Açık ki, sonsuz bir tanım dizisinden uzak durmamız gerekiyor. Bu da bizi bazı terimleri tanımlanmamış bırakmaya zorlar. Tabi ki, hala aklımızdakini sezgisel biçimde ifade edebiliriz ancak bu sezgisel tanımlama teorimizin bir parçası olmak zorunda değildir.

Listedeki 2 numaralı eleman olan aksiyomların da biraz açıklanmaya ihtiyacı var. Matematiksel bir teorideki bütün terimleri tanımlayamadığımız gibi aynı sebeple teorideki her ifadeyi de kanıtlayamayız. Bir yerden başlamak için kanıtlanmayacak bazı ifadelere ihtiyaç vardır. Bu ifadelere **aksiyom** denir. Aksiyomlar teorinin temel özelliklerini temsil ederler.

Bilmek gerekir ki, aksiyomların doğruluğundan veya yanlışlığından söz edilmez; onlar sadece teorinin ilerleyebilmesini sağlayan tanımlanmamış terimler hakkındaki ifadelerdir. Öte yandan kendi aralarında tutarlı olmalıdırlar ve aynı anda hepsinin doğru olma imkânı olmalıdır. Kendi aralarında çelişen aksiyomlar kabul edilemez. Matematiksel bir ifadeyi uygulamaya gelince, tanımlanmamış terimler yorumlanırlar ve aksiyomlar doğru veya yanlış şeklinde önermeler haline gelir.

Bir aksiyomatik teori tanımlar yaparak ve teorem ispatlanarak gelişir. Tanımlar, tanımlanmamış terimlerin yanlış şeylerle ilişkilendirilmemeleri için yapılırlar. Teorem ise birinci bölümde anlatılan mantıksal yargıları kullanan aksiyomları takip eden, sistemdeki çeşitli terimler hakkındaki ifadelerdir. Teorem orijinal aksiyomlardan gittikçe uzaklaşarak yayılır fakat sonuçta onlar üzerine inşa edilir. Teoremler ve ispatları saf matematiğin kalbini oluşturur.

1.2.2 İspat Yöntemleri

Görüldüğü gibi, resmi matematik, aksiyomatik yöntem üzerine inşa edilmiştir. Tanımlanmamış terimler ve aksiyomlar ile başlar, mantık kurallarını kullanarak teoremleri ispatlayarak gelişir. Bu bölümde ispatın temel özellikleri ve bazı ispat yöntemlerinin genel yapısından bahsedilecektir.

Diyelim ki, $A_1, A_2, \ldots A_n$ bir aksiyom sistemi verildi. Teorem, aksiyomların birleşimi ile mantıksal olarak anlamlandırılan sistem terimleri hakkındaki ifadelerdir. Bu sebeple, sistem içindeki bir teoremi resmi olarak bir T önermesi şeklinde öyle ki;

$$(A_1 \wedge A_2 \wedge \ldots \wedge A_n) \vdash T.$$

Hatırlarsak $P \vdash Q$, P' nin doğru olduğu her durumda doğrudur. Aksiyom sisteminin herhangi bir modelinde aksiyomlar doğru önermeler şeklinde yorumlara sahiptir böylece her teorem doğru önerme şeklinde bir yoruma sahiptir. Bu nedenle teoremler, aksiyom sistemindeki her modelde doğru olan önermelerdir.

O halde bir teoremin ispatını ne oluşturur? Gayri resmi olarak ispat, sonucu teorem olan mantıklı düşüncelerdir. Bir teorem bir kez ispat edildiğinde diğer teoremlerin ispatı için diğer aksiyomlar ile birlikte kullanılabilir. Bundan dolayı, A_i (i=1,2, …,n) aksiyomlar; T_j (j=1,2,…m) ispatlanmış teoremler olmak üzere T teoremini ispat etmek için

$$(A_1 \wedge A_2 \wedge \ldots \wedge A_n \wedge T_1 \wedge T_2 \wedge \ldots \wedge T_m) \vdash T$$

olduğunu göstermek gerekir. Bunu aksiyomların doğruluğunu varsayarak ve bunun T' nin doğruluğunu garantilediğini göstererek yaparız.

1.2.3 Koşullu Önermelerin Doğrudan İspatı

Birçok matematiksel varsayım koşullu önerme (P→Q) biçiminde ifade edilebilir. Bu sebeple bunların ispatları A_i ve T_j aksiyomlar ve teoremler olmak üzere

$$(A_1 \wedge A_2 \wedge \ldots \wedge A_n \wedge T_1 \wedge T_2 \wedge \ldots \wedge T_m) \vdash (P \rightarrow Q)$$

olduğunu göstermeyi içerir. Bu

$$(A_1 \wedge A_2 \wedge \ldots \wedge A_n \wedge T_1 \wedge T_2 \wedge \ldots \wedge T_m) \rightarrow (P \rightarrow Q)$$

ifadesinin bir tutoloji olduğunu ve $R \rightarrow (P \rightarrow Q)$ ve $(R \wedge P) \rightarrow Q$ mantıksal eşdeğerliliğini kullanarak

$$(A_1 \wedge A_2 \wedge \ldots \wedge A_n \wedge T_1 \wedge T_2 \wedge \ldots \wedge T_m \wedge P) \rightarrow Q$$

ifadesinin bir tutoloji olduğunu veya

$$(A_1 \wedge A_2 \wedge \ldots \wedge A_n \wedge T_1 \wedge T_2 \wedge \ldots \wedge T_m \wedge P) \vdash Q$$

olduğunu göstermeye denktir. O halde, P→Q şeklindeki teoremlerin doğrudan ispatı için aksiyomların doğruluğunu ve bundan dolayı tüm ispatlanmış teoremlerin doğruluğunu varsayarız.

Örnek 1.9: Tüm n tamsayıları için, n çift ise n^2'nin de çift olduğunu kanıtlayınız.

İspat: n çift bir tamsayı olsun. Bu halde 2, n'in çarpanlarından biridir ve n, m bir tamsayı olmak üzere n=2m şeklinde ifade edilebilir. Buradan yola çıkarak $n^2=(2m)^2=4m^2$ olur. $4m^2$ ifadesi $2m^2$ tamsayı olmak üzere $2(2m^2)$ şeklinde yazılabilir. Bu sebeple n^2 çifttir.

Dikkat edilirse birçok adımda sebepler göz ardı edilmiştir. Örneğin, $(2m)^2=4m^2$ eşitliğinin herhangi bir sebep belirtilmedi. Bunun nedeni bu adımın çok açık olması.Öte yandan ciddi bir ispatta eksik detaylar sağlanmalıdır.

1.2.4 Koşullu Önermelerin Ters Pozitif(contrapositive) Kullanarak İspatı

Hatırlarsak ters pozitif $\overline{Q} \rightarrow \overline{P}$, P→Q koşullu önermesi ile mantıksal eşdeğerdir. Bu nedenle, ters pozitifin doğruluğunu sağlarsak koşullu önermenin de doğru olduğu sonucuna varabiliriz. Bu da $\overline{Q} \rightarrow \overline{P}$ 'nun kendisi de koşullu bir önerme olduğundan direkt ispatını kullanabilmemize rağmen P→Q 'nun dolaylı ispatını oluşturur.

Örnek 1.10: Ters pozitifini sağlayarak, her n tamsayısı için **n^2 çift ise n de çifttir** ifadesini ispatlayınız.

İspat: İspatlanacak ifade P(n) 'n^2 çifttir', Q(n) 'n çifttir' ve n seçilmiş bir tamsayı olmak üzere, P(n) → Q(n)' dir. Ters pozitif ise ~Q(n) →~P(n): n tek ise n^2 tektir. Bu ifadeyi 'n tektir' in doğru olduğunu varsayarak ve n^2 'nin tek olduğunu göstererek kanıtlayabiliriz.

n tek bir tamsayı olsun.

$n=2m+1$ m tamsayı

$\Rightarrow$ $n^2=(2m+1)^2$

$=4m^2+4m+1$

$=2(2m^2+2m)+1$ $(2m^2+ 2m)$ tamsayı

$\Rightarrow$ n^2 tektir.

Örnek 1.11: m ve n birer pozitif tamsayı ve mn=100 ise, $m \leq 10$ veya $n \leq 10$ olduğunu ispatlayınız.

İspat: P(m,n), 'm ve n, mn=100 olan iki rastgele pozitif tamsayı' ve Q(m,n), '$m \leq 10$' ve '$n \leq 10$' önermelerinin dahili birleşimi olmak üzere P(m,n) →Q(m,n) olduğunu göstermek gerekir.

De Morgan kuralından $\overline{(p \vee q)} \equiv \overline{p} \wedge \overline{q}$ böylece Q(m,n)'nin tersi 'm>10' ve 'n>10' dur. Ters pozitif ~Q(m,n) →~P(m,n), bu nedenle 'm ve n rastgele tamsayılar olmak üzere m>10 ve n>10 ise mn≠100'.

m ve n pozitif tamsayılar olsun. Böylece,

m>10 ve n>10

⇒ mn>100

⇒ mn≠100

Böylece teorem ispatlanmış olur.

1.2.5 Çelişki(contradiction) ile İspat

Bir doğruluk tablosu kullanarak f bir çelişki olmak üzere P ve $\overline{P} \rightarrow f$ ' nin mantıksal eşdeğerliklerini kolayca sağlayabiliriz. Bu sebeple T teoremini ispatlamak için bunun yerine $\overline{T} \rightarrow f$ koşullu önermesini ispat edebiliriz. Bu da aksiyomların ve teoremlerin ve de $\overline{T}$' nün doğruluğu (T' nin yanlışlığı) varsayılarak gerçekleştirilebilir. Daha sonra bunun daima yanlış olan bir önerme yani bir çelişki anlamına geldiğini gösterebiliriz. Çoğunlukla, çelişki bir önerme ve tersinin kesişimi $Q \wedge \overline{Q}$ şeklindedir. $\overline{T} \rightarrow f$ 'nin doğru olduğu sonucuna varabiliriz ve bu nedenle T teoremi doğrudur.

Örnek 1.12: $\sqrt{2}$ 'nin rasyonel olmadığını ispatlayınız.(p ve q tamsayı ve q≠0 olmak üzere p/q biçiminde yazılabilen tamsayılara rasyonel sayı denir.)

İspat: Bu teoremin ispatı çelişki ile ispatlamanın bilinen bir örneğidir. $\sqrt{2}$ nin rasyonel olduğunu varsayarak bunun bir çelişkiye neden olduğunu göstermemiz gerekir.

Diyelim ki, $\sqrt{2}$ rasyonel bir sayı ve m ile n tamsayı ve n≠0 olmak üzere $\sqrt{2}$ =m/n. m/n kesrinin en sadeleşmiş halinde yani m ve n'nin ortak çarpanlarının olmadığını varsayabiliriz. Eğer ortak çarpanları varsa sadeleştiririz. Şimdi,

$\sqrt{2}$ =m/n

⇒ $2=m^2/n^2$

⇒ $2n^2=m^2$

⇒ m^2 çifttir.

⇒ m çifttir. (Örnek 1.9)

⇒ m=2p herhangi bir p tamsayısı için

⇒ $m^2=4p^2$.

Bu sonucu $2n^2=4p^2$ eşitliğinde yerine koyarsak,

$2n^2=4p^2$

⇒ $n^2=2p^2$

⇒ n^2 çifttir

⇒ n çifttir.

Böylece hem m hem de n'nin çift olduğunu yani 2'nin ortak çarpan olduğunu göstermiş olduk. Ancak m ve n hiçbir ortak çarpana sahip değildi çünkü böyle bir çarpan en başta sadeleştirildi. Bu nedenle bir önerme ve tersinin birleşimini yani bir çelişkiyi ortaya çıkardık ve bu da teoremi ispatlamaktadır.

1.2.6 Çift Yönlü koşullu Önermelerin İspatı

Çift yönlü bir önermeyi $P \leftrightarrow Q$, ispat etmek için genellikle $P \leftrightarrow Q$ ve $[(P \rightarrow Q) \wedge (Q \rightarrow P)]$' nin mantıksal eşdeğerliliğine başvururuz. Bu nedenle çift yönlü koşullu önermelerin ispatı iki ayrı bölüm içerir: biri $P \rightarrow Q$'yu diğeri $Q \rightarrow P$' yi ispatlamak.

Örnek 1.13: Herhangi x ve y tamsayıları için xy çarpımının, sadece ve sadece 'x çiftse' veya 'y çiftse' çift olduğunu ispatlayınız.

İspat: Önce direkt ispat kullanarak x çiftse veya y çiftse xy' nin çift olduğunu kanıtlarız.

x çift olsun. Örneğin n bir tamsayı olmak üzere x=2n. O halde xy=2ny yani xy çifttir. Eğer y çift olsaydı benzer bir kanıt xy' nin çift olduğunu gösterebilir.

Şimdi tersini ispatlayalım: Eğer xy çift ise x çifttir veya y çifttir. Bunun için ters pozitifin direkt ispatını kullanabiliriz: x ve y tek ise xy de tektir.

O halde x ve y tek olsun.

$\Rightarrow$ $x=2n+1,\ y=2m+1$ m ve n tamsayı olmak üzere

Öyleyse $xy=(2n+1)(2m+1)$

$=4mn+2n+2m+1$

$=2(2mn+n+m)+1$

$\Rightarrow$ xy tektir. Bu da ispat demektir.

1.2.7 Aksine Örneklerin Kullanımı

Birçok matematiksel konjektür 'tüm A lar B dir' veya 'A özelliğine sahip tüm nesneler B özelliğine sahiptir' biçimindedir. Bu şu şekilde de yazılabilir: A(x) 'x, A dır(A özelliğine sahiptir)' ve B(x) 'x B dir (B özelliğine sahiptir)' olmak üzere $(\forall x)[A(x) \rightarrow B(x)]$.

Önerme şu şekilde de yazılabilir: x A evreni ile sınırlandırılmış olmak üzere $(\forall x)[B(x)]$. Daha önce söylenildiği gibi B özelliğine sahip olmayan bir x bulamamak teoremin ispatını oluşturmaz. Öte yandan B özelliğine sahip birçok x bulmak da bu özelliğe sahip olmayan x bulamayacağımızı garanti etmez. Ancak, evren sonlu bir evrense ve yeterli zaman varsa bütün elemanları kontrol edip özelliğin olup olmadığı sorusunun cevabını bulabiliriz. Eğer tüm elemanlarda bu özellik varsa teorem ispatlanmış olur. Bu yönteme **tüketme ile ispat** denir çünkü x' in bütün olasılıkları tüketilir.

Diğer yandan, $(\forall x)[B(x)]$ biçiminde bir konjektürün yanlış olduğunu ispat etmek için evrendeki sadece bir üyenin B özelliğine sahip olmadığını bulmamız gerekir. Bu aksine örnekle ispatın esasıdır.

1.2.8 Matematiksel İndüksiyon

Aslında matematiksel indüksiyon diye bilinen ispat yöntemi tümevarımsal bir ispat değildir. Olmamasının nedeni kabul edilen ispatlar sadece tümdengelimsel yargılar(insanlar

ölümlüdür, Ali insandır, Öyleyse Ali ölümlüdür) barındırır. İndüksiyonun doğruya yakın olan bilgiyi ve bundan sonra makul tahmini sağlama görevi vardır. Herhangi bir ispatla ilgili problem, onu ispatlamadan önce sonucu bilmemiz gerektiğidir.

Birçok matematiksel konjektür pozitif tamsayıların özellikleri ile ilgilidir. Örneğin şu problem: ilk n tek tamsayının toplamı için bir formül bulun. Başlama noktası olarak n' in küçük değerleri için toplamı yazmak ve bunun bize olası konjektür hakkında bir fikir verip vermediğini gözlemektir.

n=1 için, toplam 1' dir.
n=2 için, toplam 1+3=4' tür.
n=3 için, toplam 1+3+5=9' dur.
n=4 için, toplam 1+3+5+7=16' dır.

Bu aşamada n' in her değeri için toplamın n^2 olduğunu fark ederiz. Birkaç tane daha deneyip daha da emin olmak isteriz.

n=5 için, toplam 16+9=25' dur.
n=6 için, toplam 25+11=36' dır.

Tümevarımsal yargı bizi ilk n tek tamsayının toplamı n^2'dir konjektürüne götürür. Bunun tüm pozitif n tamsayıları için doğru olduğunu tümdengelime dayanarak ispatlamalıyız.

Matematiksel indüksiyon sonucun tüm pozitif tamsayılar için geçerli olduğunu ispatlamak için uygundur ve şu adımları içerir:

(a) Konjektürün n=1 için geçerli olduğunu ispatla
(b) Her $k \geq 1$ için, eğer sonuç n=k için sağlanıyorsa n=k+1 için de sağlanmalıdır. Bu adım tümevarımsal adım olarak bilinir.

(b) şıkkındaki koşullu önermeyi ispatlamak için bir önceki konuda anlatılan teknikler kullanılır. Öte yandan, tümevarımsal adım genellikle direkt ispat kullanılarak sağlanır. Sonucun n=k için sağlandığını varsayarız. (Bu varsayım bazen tümevarımsal hipotez şeklinde adlandırılır.) Bundan n=k+1 için de sağlandığı sonucunu çıkarırız. n=1 için sağlandığına göre tümevarımsal adım bizi n=2, n=3 vs. için de sağladığı sonucuna götürür. Matematiksel indüksiyonun prensibi, sonucun tüm n pozitif tamsayıları için sağlandığını gösterir.

Örnek 1.14: İlk n tane pozitif tek tamsayının toplamının n^2 olduğunu ispatlayınız.

İspat: İspatlamak istediğimiz şey: $\underbrace{1 + 3 + 5 + \ldots}_{\longleftarrow \text{n terms} \longrightarrow} = n^2$.

Dizideki son eleman 2n-1 'dir ve bu nedenle konjektürümüzü şu şekilde yazabiliriz:

$$1 + 3 + 5 + \ldots + (2n-1) = n^2.$$

Daha sonra aşağıdaki adımları izleriz.

(a) Konjektürün n=1 için doğru olduğunu ispatla.

n=1 için, $1=n^2$. O halde n=1 için konjektür doğrudur.

(b) $k \geq 1$ olmak üzere konjektürün n=k için doğru olduğunu varsay ve bunun n=k+1 için konjektürün doğruluğuna yol açtığını göster.

Varsayalım ki, $1 + 3 + 5 + \ldots + (2k-1) = k^2$. Bir sonraki tamsayı olan 2k+1'i eşitliğin iki tarafına eklersek,

$$1 + 3 + 5 + \ldots + (2k-1) + (2k+1) = k^2+(2k+1)$$
$$=(k+1)^2.$$

Bu eşitliğin sol tarafı ilk k+1 tane tek tamsayının toplamıdır ve tümevarımsal hipotezi kullanarak gösterdik ki, bu toplam $(k+1)^2$'dir. Böylece konjektürün eğer n=k için sağlanıyorsa, n=k+1 için de sağlandığını göstermiş olduk. Ayrıca n=1 için de sağlandığını gösterdik ve matematiksel indüksiyon kuralına dayanarak teorem tüm pozitif n tamsayıları için sağlanır diyebiliriz.

1.2.9 Matematiksel İndüksiyon Prensibinin değişimleri

Tümevarımsal prensip üzerinde değişik modifikasyonlar yapılabilir. Örneğin, S(n) önermesinin sabit bir N tamsayısından büyük veya eşit tüm tamsayılar için sağlandığını ispat etmek isteyelim. Tümevarım prensibi üzerinde bazı modifikasyonlar yaparsak şunu elde ederiz:

(a) S(N)' in doğru olduğunu ispatla.
(b) $k \geq N$' yi sağlayan her tamsayı için, eğer S(k) doğru ise S(k+1) de doğrudur.

Bu tümevarım ile ispatın standart metodudur sadece 1 yerine N ile başlanmıştır.

Tümevarımsal ispatın daha önemli bir modifikasyonu 'indüksiyonun ikinci prensibi' ile sağlanır. Bunun önemi şudur: Tümevarımsal adıma geldiğimizde S(k)' nin sadece k yerine, k' dan küçük ve eşit tüm pozitif r tamsayıları için doğru olduğunu varsayarız.

İndüksiyonun İkinci Prensibi

S(n) doğal n sayısı ile ilgili bir ifade ve q sabit bir doğal sayı olsun. S(n) 'in tüm $n \geq q$ için doğruluğunun indüksiyon ile ispatı için adımlar;

(a) Temel adım :S(q) nin doğruluğunu ispatla ve,
(b) eğer $k \geq q$ için, S(q), S(q+1), S(q+2),…., S(k) doğru ise (tüm $q \leq k$ için S(q)' nin doğruluğu S(k+1)'in doğruluğu anlamına gelir.

İndüksiyonun bu ikinci prensibi ilk başta ilkinden daha genel gibi gözükür çünkü S(k+1)'in doğru olduğu sonucuna varmak için daha fazla varsayımda bulunuruz. Ancak, 'S(q), $q \leq k$' yı sağlayan tüm pozitif tamsayılar için doğrudur' önermesine T(n) dersek, ikinci prensibin iki kısmı:

(a) T(q) doğrudur, ve
(b) $k \geq q$ için T(q)'nin doğruluğu T(k+1)'in doğruluğu anlamına gelir.

Bu durumda indüksiyonun ikinci adımında öncekine göre daha fazla bilgi gerekir. Buna indüksiyonun kuvvetli prensibi denir. Bu şekle **tam indüksiyon** denir.

Örnek 1.15: birden büyük olan herhangi bir doğal sayının asal sayıların çarpımı şeklinde gösterilebileceğini ispatlayın.

S(n) , n, birden büyük doğal sayı ise n'in asal sayıların çarpımı olduğunu indüksiyon ile tüm n'ler için gösterelim.

a)Temel adım. S(2) için doğru. 2 asal sayıların çarpımı şeklinde gösterilebilir

b) İndüksiyon adımı: S(2), S(3), …… ,S(k) nın doğruluğu S(k+1)'in doğruluğunu kanıtlar. Şimdi eğer k+1 asal sayı ise doğrudur , eğer k+1 asal sayı değil ise m,n <k olmak üzere k=m.n şeklinde gösterilebilir. İndüksiyon adımı ile m ve n 'nin her ikisi de asal sayıların çarpımı olarak gösterilebilir.. Böylece k+1 asal sayıların çarpımı olarak gösterilebilir.

1.2.10 Tümevarımsal Tanımlar (Kümelerin ve fonksiyonların, yinelemeli(rekürsif) tanımları)

Tümevarımsal prensibin kullanımı sadece pozitif tamsayılar hakkındaki önermelerin ispatı ile sınırlandırılmamıştır; matematiksel nesnelerin ve özelliklerin tanımı için de kullanılırlar. Bazı durumlarda nesnelerin açık olarak tanımlanması zordur. Bu durumlarda nesneler kendileri cinsinden tanımlanırlar. Böyle tanımlamaya yinelemeli(rekürsif) tanımamla denir. Yinelemeli tanım, seri, fonksiyon ve kümelerin tanımında kullanılabilir. Örnek olarak, $a_n = 2^n$ (n=0,1,2, ……) olarak verilen 2'nin kuvvetleri dizisi verilsin. Bu diziyi ilk terimi $a_0 = 1$ ve sonraki elemanların öncekiler cinsinden tanımı için bir kural vererek $a_{n+1} = 2.a_n$ (n=0,1,2, ……) şeklinde tanımlanır.

Kümelerin tümevarımla tanımlanması bazı problemlerin çözümünü kolaylaştırır. Bu tanıma indüktif veya yinelemeli(recursive) tanımlama denir. Bir kümenin yinelemeli tanımı üç adımdan oluşur.

1. Temel adım. Tanımlanacak kümenin belirli elemanı kümeye ait olduğu ifade edilir.
2. İndüktif(yinelemeli) adım. Bu adımda kümenin içindeki mevcut elemanları kullanarak kümenin daha fazla eleman bulundurabileceğini söyler.
3. Kapalı parça. Kümenin içinde 1ve 2 adımda tanımlanan elemanlar olduğunu söyler.

Örnek 1.16.: 5 ile bölünebilen tamsayılardan oluşan A kümesinin tanımı aşağıdaki adımlardan oluşur.

a) 5 sayısı A'nın bir elemanıdır.
b) Eğer n , A'nın elemanı ise, n+5'de A'nın elemanıdır.
c) A'daki bir nesne ancak ve ancak (a) ve (b) adımlarının tekrarlanmasıyla elde edilebilir.

Fonksiyonların yinelemeli tanımı: Eğer bir fonksiyon f(n) ondan önce gelen elemanlar f(i) ler cinsinden tanımlanıyorsa buna yinelemeli(rekürsif) tanım denir. f(0),f(1),f(2),…, f(k)'ya da başlangıç değerleri denir. Bir başka ifade ile;

a) Fonksiyonun sıfırdaki değerini ata.
b) Fonksiyonun değerini bir tamsayı olarak hesaplayan ve kendisinden küçük sayılar cinsinden ifade eden bir kural tanımla.

Örnek 1.17: F(n) =n! Faktöriyel fonksiyonunu yinelemeli olarak tanımlayalım.

a) fonksiyonun sıfırdaki değeri F(0) = 1
b) F(n+1) 'i F(n) cinsinden hesaplayan kural , (n+1)! 'in n!'den hesaplanabilmesi (n+1) ile çarpılarak olacaktır. Bu durumda kural:

F(n+1)=(n+1).F(n) şeklinde olacaktır.

Aşağıdaki Fibonacci sayıları dizisini ele alırsak:

1, 1, 2, 3, 5, 8, 13, 21,…

Dizideki her bir sayı kendinden önceki iki sayının toplamıdır. f_n n. Fibonacci sayısını

temsil ediyorsa, diziyi şu şekilde tanımlayabiliriz:

$f_1 = 1, f_2 = 1$ ve $n \geq 3$ için, $f_n = f_{n-1} + f_{n-2}$

Fark edileceği gibi tümevarımsal tanım indüksiyon prensiplerine uymaz. Tümevarımsal tanıma başlamak için, ilk iki Fibonacci sayısını tanımlamamız gerekir, sadece ilkini değil. Aşağıda pozitif n tamsayısına dayanan A_n matematiksel nesne ve özelliğine ait tümevarımsal tanımın genel formu gösterilmiştir.

Tüm pozitif tamsayılar için A_n 'i tanımlamak için:

(a) k=1,2,…r için ayrı ayrı A_k'yi tanımla

(b) k>r için A_k'yi $A_1, \ldots A_{k-1}$ biçiminde tanımla

Bazı nesneleri veya tümevarımsal olarak tanımlanmış bazı özellikleri içeren önermeleri ispatlamak için matematiksel indüksiyonu kullanmak doğaldır.

1.3 Küme Teorisi

1.3.1 Kümeler ve Üyeler

Küme notasyonu matematikteki temel kavramlardan biridir. Bir kümenin kusursuz bir tanımı burada verilmeyecektir zira küme teorisine göre küme çoğunlukla tanımsızdır. Ancak bu terimle ne demek istediğimizi açıklayabiliriz: hangi tip olursa olsun objeler topluluğu küme olarak düşünülür. Objeler her şey olabilir ve bunlara kümenin elemanları denir. Bir kümedeki elemanların ortak özelliği olmasına gerek yoktur (aslında en bariz ortak noktaları aynı küme içinde bulunmalarıdır). Benzer şekilde eleman sayısında da belli bir kısıtlama yoktur; sonsuz sayıda, sonlu sayıda veya hiç eleman olmayabilir. Diğer yandan tek bir sınırlama vardır: verilen bir küme ve obje ile objenin kümenin elemanı olup olmadığına karar verebilmemiz gerekir.

Örnek 1.18:

1. Bir küme Picasso' yu, Eyfel Kulesini ve π sayısını içerecek şekilde tanımlanmış olabilir. Bu (biraz garip olsa da) sonlu bir kümedir.

2. Tüm pozitif çift tamsayıları içeren küme açıkça sonsuz bir kümedir.

3. Gelmiş geçmiş en iyi 10 şarkıyı içeren kümeyi düşünelim. Eğer en iyinin tanımını vermezsek bu küme geçerli bir küme olmaz. Kime göre en iyi? Bu tanım bir elemanın bir kümenin elemanı olup olmadığına karar verebilmemiz koşuluna uymaz.

1.3.2 Notasyon

Genellikle kümeleri ifade etmek için büyük harfler, elemanları ifade etmek için küçük harfler kullanılır. $\in$ sembolü '-e ait' veya '-nin elemanıdır' anlamına gelir. Bu nedenle

$\alpha \in A$ 'nın anlamı α elemanı A kümesine aittir ve

$\alpha \notin A$ 'nın anlamı $\sim(\alpha \in A)$ veya α A'ya ait değildir.

1.3.3 Kümeleri Tanımlamak

Kümeler değişik biçimlerde tanımlanabilir. En basiti elemanları köşeli parantezler {} arasına listelemektir. Örnek 1.18' deki iki kümeyi bir daha yazarsak:

A={Picasso, Eyfel Kulesi, π }

B={2,4,6,8…..}

İkinci kümede bütün elemanları listelemeyiz. Bu yüzden '…' kullanarak listenin daha böyle devam ettiğini belirtiriz. Diğer küme gösterim örnekleri şunlardır:

Sabit bir pozitif n tamsayısı için, C_n={1,2,…n}, ilk n pozitif tamsayının kümesidir. Yine sonlu sayıda olmasına rağmen arada birçok elemanın var olduğunu göstermek için '…' kullandık.

D={}, **boş küme**dir yani hiçbir elemanı yoktur. Bu küme genellikle $\varnothing$ ile gösterilir.

Bir kümenin elemanlarını listelemek küçük veya belli bir kalıba sahip elemanlı kümeler haricinde pek pratik değildir. Alternatif bir yol küme elemanlarını bir özellik ile tanımlamaktır. Daha açık bir ifadeyle, P(x) tek değişkenli bir önermesel fonksiyon ise elemanları, α için P(α)'nın doğru bir önerme olduğu tüm α objeleri olan kümeyi oluşturabiliriz.

Bu şekilde tanımlanan bir küme; A={x:P(x)} şeklinde ifade edilir. (Bu şu şekilde okunur: P(x)' i sağlayan tüm x'lerin kümesi)

1.3.4 Kümelerin Eşitliği

İki küme sadece ve sadece aynı elemanları içeriyorsa eşit olarak tanımlanır; şöyle ki, eğer $(\forall x)\left[x \in A \leftrightarrow x \in B\right]$ doğru ise A=B' dir yada tersi. Listelenen elemanların sırası önemsizdir.

Şunu da unutmamak gerekir ki; sadece bir boş küme vardır veya tüm boş kümeler eşittir. Çünkü tüm boş kümeler aynı elemanı içerir yani hiçbir elemanı.

Ayrıca, eğer P(x) ve Q(x) aynı x objeleri için doğru olan önermesel fonksiyonlar ise tanımladıkları kümeler eşittir.

$$\{x:P(x)\}=\{x:Q(x)\}.$$

Tanım: Eğer A sonlu bir küme ise kardinalitesi, |A|, içerdiği (farklı) elemanların sayısıdır.

Eğer A sonsuz sayıda elemana sahipse, sonsuz kardinalitesi vardır deriz ve şu şekilde ifade ederiz: |A|=∞.

A' nın kardinalitesi için kullanılan diğer notasyonlar n(A), #(A) ve $\overline{\overline{A}}$.

Örnek 1.19:

1. $|\varnothing|$=0 çünkü $\varnothing$' nın hiç elemanı yoktur.
2. |{ π ,2,Einstein}|=3.
3. Eğer X={0,1,……..,n} ise |X|=n+1.
4. |{2,4,6,8,…..}| = ∞

Kardinalite basit bir kavram gibi görünse de verilen bir kümenin kardinalitesini hesaplamak bazen pratikte zor olabilir. Bu durum genellikle verilen kümenin elemanlarından bazıları

kendileri birer küme olduğunda gerçekleşir. Küme elemanlarının kendi başlarına bir küme olması geçerli bir yapıdır.

Örneğin, X={{1,2}} olsun. Bu durumda X sadece tek bir eleman içerir yani {1,2} kümesini ve |X|=1' dir. Kardinalitesi 2 olan {1,2} kümesi ile tek elemanı {1,2} kümesi olan X kümesini ayırt etmek son derece önemlidir. Benzer şekilde $\varnothing$ ve $\{\varnothing\}$ kümeleri de farklıdır zira $|\{\varnothing\}|$=1' dir.

Örnek 1.20: $|\{1,2,\{1,2\}\}|=3$,

$|\{\varnothing,\{1,2\}\}|=2$,

$|\{\varnothing,\{\varnothing\}\}|=2$,

$|\{\varnothing,\{\varnothing\},\{1,2\}\}|=3$,

$|\{\varnothing,\{\varnothing,\{\varnothing\}\}\}|=2$.

1.3.5 Alt Kümeler

Tanım: A' nın tüm elemanları aynı zamanda B' nin de elemanları ise A kümesi B kümesinin alt kümesidir denir ve A$\subseteq$B şeklinde gösterilir. Sembolik olarak, $(\forall x)[x \in A \rightarrow x \in B]$ ise A$\subseteq$B' dir.

Eğer A B' nin alt kümesi ise B, A 'nın süper kümesidir (superset) veya kapsar deriz ve B$\supseteq$A yazarız. A$\subset$B notasyonu 'A, B 'nin tam alt kümesidir' ifadesi için kullanılır. Bu nedenle sadece ve sadece A$\subseteq$B ve A$\neq$B ise A$\subset$B' dir. Ayrıca tüm A kümeleri için $\varnothing \subseteq$A' dir.

İki kümenin eşit olduğunu kanıtlamak için her birinin diğerinin alt kümesi olduğunu göstermek yeterlidir. Esasen bu, aşağıdaki bileşik önemelerin mantıksal eşdeğerliliğinden kaynaklanır.

$$[(p \rightarrow q) \wedge (q \rightarrow p)] \equiv (p \leftrightarrow q).$$

Alt kümenin tanımı ile A$\subseteq$B' nin anlamı $(\forall x)[x \in A \rightarrow x \in B]$ doğrudur ve B$\subseteq$A 'nin anlamı $(\forall x)[x \in B \rightarrow x \in A]$ doğrudur, bu durumda A$\subseteq$B ve B$\subseteq$A sadece ve sadece $(\forall x)[x \in A \rightarrow x \in B] \wedge (\forall x)[x \in B \rightarrow x \in A]$ ise doğrudur. $(\forall x)[x \in A \rightarrow x \in B]$' nin ve $(\forall x)[x \in B \rightarrow x \in A]$' nin doğruluğu $(\forall x)[x \in A \leftrightarrow x \in B]$'nin doğruluğunu garantiler ve tam tersi. Bu sebeple, A=B olduğu zaman A$\subseteq$B ve B$\subseteq$A ifadelerinin ikisi de doğrudur. Özet olarak:

Teorem 1.1: İki küme; A ve B sadece ve sadece A$\subseteq$B ve B$\subseteq$A ise eşittir.

Örnek 1.21: A={{1},{2},{1,2}} ve B, {1,2}' nin boş olmayan tüm alt kümeleri olsun. A=B olduğunu gösteriniz.

Çözüm: A$\subseteq$B 'dir çünkü A' nın 3 elemanının her biri {1,2}'nin boş olmayan alt kümesidir ve bu nedenle B' nin bir elemanıdır.

B$\subseteq$A' dır çünkü {1,2}' nin boş olmayan tüm alt kümeleri A' da yer alır. Yukarıdaki teoremi kullanarak A=B sonucuna varabiliriz.

Evrensel Küme: Küme kavramı çok geniş olduğundan çoğunlukla belirli kontekst için gerekli olan kümelere önem verilir. Mevcut görevi veya çalışmayı ilgilendiren kümeleri içine alan küme **evrensel küme** olarak tanımlanır. Evrensel kümenin dışında kalan her şey göz ardı edilir. Evrensel küme her zaman için sabit olan bir şey değildir- kontekste göre değişir.

Evrensel küme olarak kullanılan bazı özel sayı kümeleri aşağıdadır.

N= {0,1,2,3,….} doğal sayılar kümesi.

Z= {…, -2,-1,0,1,2,…} tam sayılar kümesi.

Q= $\{p/q : p,q \in Z$ ve $q \neq 0\}$ rasyonel sayılar kümesi.

R = reel sayılar kümesi; reel sayılar sayı doğrusu üzerindeki noktalar veya ondalık şeklinde yazılan sayılar şeklinde düşünülebilir.

C=$\{x+iy : x,y \in$ R ve $i^2=-1\}$ karmaşık sayılar kümesi.

Açıkça görüldüğü gibi bu kümeler arasında şu alt küme ilişkileri vardır:

$$N \subseteq Z \subseteq Q \subseteq R \subseteq C.$$

Ayrıca Z^+, Q^+ ve R^+ sırasıyla pozitif tamsayıları, rasyonel sayıları ve reel sayıları ifade etmek için kullanılır. Dikkat edilirse N, Z^+ 'ya eşit değildir zira 0 ilkine dahil olmasına rağmen ikincisine değildir. Ek olarak, bazen çift ve tek sayıları ifade etmek için E ve O'yu kullanırız:

$$E=\{2n : n \in Z\}=\{\ldots,-4,-2,0,2,4,\ldots\}$$

$$O=\{2n+1 : n \in Z\}=\{\ldots,-3,-1,1,3,\ldots\}.$$

Eğer evrensel bir küme {x:P(x)} notasyonu ile tanımlanmış ise bunun anlamı P(x)'i sağlayan evrensel kümedeki tüm x' lerin kümesidir. Bu nedenle eğer mevcut evrensel kümemiz Z ise X=$\{x : 2x^2+3x-2=0\}$, {-2} kümesidir fakat *U,* Q veya R ise X={-2,1/2}. İlk durumda sınırlandırmayı daha belirgin yapabilirdik ve şekilde yazabilirdik:

$$X=\{x : x \in Z \text{ ve } 2x^2+3x-2=0\} \text{ veya } X=\{x \in Z : 2x^2+3x-2=0\}.$$

1.3.6 Kümeler Üzerinde İşlemler

Venn şeması kümelerin yararlı bir görsel gösterimidir. Böyle bir şemada kümeler, düzlemdeki bölgeler olarak temsil edilir ve verilen kümeye ait elemanlar kendisini temsil eden bölgenin içine yerleştirilir. Bazen tüm kümeler evrensel kümeyi temsil eden bir kutuya yerleştirilir. Eğer bir eleman iki kümenin birden elemanı ise iki küme iç içe çizilir ve bu elemanlar iç içe geçmiş kısma konur.

Verilen A ve B kümeleri ile aşağıdaki gibi yeni iki küme tanımlayabiliriz.

A ve B' nin **kesişimi**, A ve B' nin her ikisine birden ait olan tüm elemanların kümesidir ve $A \cap B$ şeklinde gösterilir.

A ve B' nin **birleşimi**, A' ya, B' ye veya her ikisine ait olan tüm elemanların kümesidir ve $A \cup B$ şeklinde gösterilir.

Sembolik olarak;

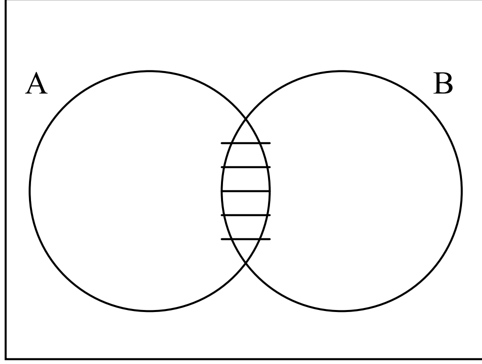
$$A \cap B=\{x : x \in A \text{ ve } x \in B\}$$
$$A \cup B=\{x : x \in A \text{ veya } x \in B \text{ veya her ikisi birden}\}.$$

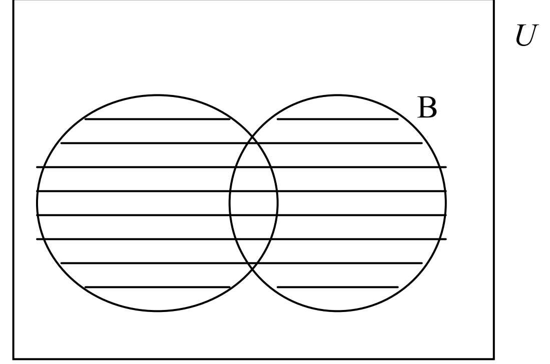
Kümelerin kesişimi ile önermelerin kesişimi arasında açık bir bağlantı vardır tıpkı kümelerin birleşimi ve önermelerin dahili birleşimi arasında olduğu gibi. Eğer A ve B, sırasıyla P(x) ve Q(x) önermesel fonksiyonları ile tanımlanmışlar ise;

$A\cap B=\{x: P(x)\wedge Q(x)\}$ ve

$A\cup B=\{x: P(x)\vee Q(x)\}$.

Bu kümeler en iyi Şekil 1.1 ve 1.2'deki Venn şemaları ile gösterilebilir. Taralı bölgeler kesişim ve birleşimi gösterir.





Şekil 1.1: $A\cap B$ **Şekil 1.2:** $A\cup B$

Kesişim ve birleşimin tanımlarını ikiden fazla kümeye genişletebiliriz. A_1, A_2, … A_n küme olsun.

Bunların kesişimi:

$$\bigcap_{r=1}^{n} A_r = A_1 \cap A_2 \cap \ldots \cap A_n$$

$= \{x: x\in A_1 \text{ ve } x\in A_2 \text{ ve … ve } x\in A_n\}$

$=\{x: x$, r=1,2,…,n olmak üzere her bir A_r kümesine aittir.}

Birleşimi ise;

$$\bigcup_{r=1}^{n} A_r = A_1 \cup A_2 \cup \ldots \cup A_n \qquad = \{x: x\in A_1 \text{ veya } x\in A_2 \text{ veya … veya } x\in A_n\}$$

$=\{x: x$, r=1,2,…,n olmak üzere en az bir A_r kümesine aittir.}

A ve B kümeleri ortak elemana sahip değilse **ayrık**tır denir yani $A\cap B=\varnothing$. Venn şemasında bu iç içe geçmemiş kümeler şeklinde gösterilir.

Verilen bir A kümesinin **tümleyeni**, A 'ya ait olmayan fakat *U*'da yer alan tüm elemanlardır. A'nın tümleyeni $\overline{A}$ (veya A') şeklinde gösterilir. Tümleyen ile tersini alma arasında açık bir ilişki vardır; eğer A={x: P(x)} ise $\overline{A}$={x: ~P(x)}' tir.

Bir kümenin tümleyeni ile bağlantılı olarak A ve B kümelerinin **farkı** A-B veya A\B şeklinde gösterilir ve bu küme A'nın B'de yer almayan tüm elemanlarını içerir:

$A\text{-}B=\{x: x\in A \text{ ve } x\notin B\}$.

A'nın tümleyeni $\overline{A}=U$-A'dır.

Örnek 1.22: $U=\{1,2,3,\ldots,10\}=\{n: n\in Z^{+}$ ve $n\leq 10\}$, $A=\{n\in U : 1\leq n<7\}$, $B=\{n\in U$: n 3'ün katları$\}$ olsun. O halde; $A=\{1,2,3,4,5,6\}$ ve $B=\{3,6,9\}$. Bu nedenle:

$$A\cap B=\{3,6\}$$

$$A\cup B=\{1,2,3,4,5,6,9\}$$

$$A-B=\{1,2,4,5\}$$

$$B-A=\{9\}$$

$$\overline{A}=\{7,8,9,10\}$$

$$\overline{B}=\{1,2,4,5,7,8,10\}$$

$$\overline{A\cup B}=\{7,8,10\}=\overline{A}\cap\overline{B}$$

$$\overline{A\cap B}=\{1,2,4,5,7,8,9,10\}=\overline{A}\cup\overline{B}$$

1.3.7 Sayma Teknikleri

Bazı karmaşık matematiksel sonuçlar sayma argümanlarının ispatlarına bağlıdır: çeşitli kümelerin eleman sayılarını saymak, belli bir sonucun kaç değişik yolla elde edilebileceğini saymak gibi. Sayma kısmen kolay bir olay gibi görünse de, pratikte çok karmaşık olabilir. Matematikçiler sayma problemleri için birçok teknik ve sonuç üretmişlerdir ve konuya sayma teorisi adını vermişlerdir.

Saymanın en basit sonuçlarından biri şudur: iki ayrık A ve B kümesinin toplam eleman sayısını bulmak için A'nın elemanlarını, B'nin elemanlarını sayıp toplarız.

Sayma Prensibi 1: Eğer A ve B ayrık iki küme ise $|A\cup B| = |A| + |B|$.

Çoğu uygulama doğal olarak ikiden fazla küme içerir. Yukarıdaki prensip aşağıdaki şekilde genelleştirilir.

Sayma Prensibi 2: Eğer $A_1, A_2, \ldots, A_n$ küme ise ve bu kümelerin hiçbir çifti ortak bir elemana sahip değilse $|A_1\cup A_2\cup\ldots\cup A_n| = |A_1|+|A_2|+\ldots+|A_n|$.

Bazen, elemanları sayılacak kümeler yukarıdaki sayma prensiplerinin katı kuralını-herhangi bir çiftin ayrık olması- sağlamayabilir. Öte yandan, bu durumda kümeyi sayma prensiplerinin koşullarını sağlayacak alt kümeler bölmek mümkündür. Bu şekilde ispatlanabilecek en basit sonuç şudur:

Teorem 1.2(Ekleme(inclusion)-Çıkarma(exclusion) Prensibi): Eğer A ve B sonlu kümeler ise $|A\cup B|=|A|+|B|-|A\cap B|$.

İspat: $A\cup B$' yi sayma prensibi 2'yi sağlayan alt kümelerine böleriz: A-B, $A\cap B$ ve B-A.

Sayma prensibi 2' den,

$$|A \cup B| = |A-B|+|A \cap B|+|B-A|. \qquad (1)$$

A ve B kümelerinin kendileri sırasıyla A-B, $A \cap B$ ve B-A, $A \cap B$ şeklinde ayrık alt kümelere bölünebilir. Böylece;

$$|A|=|A-B|+|A \cap B| \qquad (2)$$

$$|B|=|B-A|+|A \cap B|. \qquad (3)$$

Bu durumda (1), (2) ve (3) eşitliklerini birleştirerek istenilen sonucu elde etmek çok kolay bir işlemdir. Ekleme-çıkarma prensibi bu şekilde adlandırılır çünkü $A \cup B$' nin elemanlarını saymak için A'nın elemanlarını ve B'nin elemanlarını ekledik ve böylece $A \cap B$' nin elemanlarını iki kere eklemiş olduk. $A \cup B$' nin doğru eleman sayısını elde etmek için $A \cap B$'yi bir kere çıkarmamız gerekir.

İki kümeden fazla durumlar için benzer sayma teknikleri vardır. Üç küme için sonuç aşağıdaki teoremdeki gibi bulunur.

Teorem 1.3: A, B ve C sonlu kümeler ise

$$|A \cup B \cup C|=|A|+|B|+|C|-|A \cap B|-|B \cap C|-|C \cap A|+|A \cap B \cap C|.$$

1.3.8 Kümeler Cebri

Açıktır ki, kesişim, birleşim ve tümleyen işlemleri birbiriyle ilişkilidir. Örneğin;

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

Aşağıdaki kurallar tüm A, B ve C kümeleri için geçerlidir.

Aynılık (Tek Kuvvet) Özelliği

$A \cap A = A$
$A \cup A = A$.

Değişme Özelliği

$A \cap B = B \cap A$
$A \cup B = B \cup A$

Birleşme Özelliği

$A \cap (B \cap C) = (A \cap B) \cap C$
$A \cup (B \cup C) = (A \cup B) \cup C$

Yutan Eleman

$A \cap (A \cup B) = A$
$A \cup (A \cap B) = A$.

Dağılma Özelliği

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Çift ters Özelliği((Double negation)

$\overline{\overline{A}} = A.$

De Morgan Kuralları

$\left(\overline{A \cup B}\right) = \overline{A} \cap \overline{B}$

$\left(\overline{A \cap B}\right) = \overline{A} \cup \overline{B}$.

Özdeşlik Özelliği

$A \cup \varnothing = A$

$A \cap U = A$

$A \cup U = U$

$A \cap \varnothing = \varnothing$.

Tamlama Özelliği

$A \cup \overline{A} = U$

$A \cap \overline{A} = \varnothing$

$\overline{\varnothing} = U$

$\overline{U} = \varnothing$.

Bu kurallar uygun önermeler arasındaki mantıksal eşitliklerden de türetilebilmesine rağmen en iyi Venn şemaları ile gösterilir.

1.3.9 Eşlik Kuralı (Duality Principle)

$\wedge, \vee$ ve tersini alma bağlayıcılarını içeren bileşik önermelerin eşli önermeye sahip olduğu gibi $\cap, \cup$ ve tümleme içeren kümeler hakkındaki ifadeler de eşlidir. Böyle bir ifadenin eşi orijinal ifadedeki tüm $\cap$' lerin $\cup$ ile; tüm $\varnothing$' lerin U ile değiştirilmesi ile elde edilir. Örneğin;

$(A \cap \varnothing) \cup (B \cap U) \cup \overline{B} = U$ ‘in eşi $(A \cup U) \cap (B \cup \varnothing) \cap \overline{B} = \varnothing$.

Kümeler cebrinin her bir kuralının eşi de ayrıca bir kuraldır. Bunun sonucu olarak kümeler için aşağıdaki eşlik kuralı ortaya çıkmıştır.

Kümeler için eşlik kuralı: Eğer kümeler ile ilgili bir ifade tüm kümeler için doğruysa bunun eş ifadesinin de tüm kümeler için doğru olması gerekir.

1.3.10 Kümelerin Aileleri

Kümelerin ailesi veya kümlerin toplanması terimiyle, kümelerin kümesi kastedilmekte ise de her iki terimde sıklıkla kullanılmaktadır.

$I=\{1,2,\ldots,n\}$ verilsin ve $\forall i \in I$ *için,* A_i kümesi aşağıdaki şekilde tanımlanır.

$\{A_i : i \in I\} = \{A_1, A_2, \quad, A_n\}$

I kümesine gösterge kümesi denir ve Ai ‘leri birleşme için göstergeler. Eğer, $I=\{1,2,\ldots,n\}= Z^+$

ise, $\{A_i : i \in I\} = \{A_1, A_2, A_3, ...\}$ dır.

Bu notasyonu kullanarak, kümelerin keyfi bir ailesine kesişim ve birleşimi aşağıdaki şekilde tanımlanır.

$\boldsymbol{F} = \{A_i : i \in I\}$ kümelerin bir ailesi olarak verilsin burada, I herhangi bir gösterge kümesidir.

F ailesinin Kesişim ve birleşimi : $\bigcap_{i \in I} A_i = \{ x: x \in A_i$ bütün $i \in I$ için $\}$; $\bigcup_{i \in I} A_i = \{ x: x \in A_i$ bazı $i \in I$ için $\}$

Örnek: $I = Z^+ = \{1,2,3,.....,\}$ ve her bir $i \in Z^+$ için $A_i = \{i\}$. Böylece, $A_1 = \{1\}$, $A_2 = \{2\}$, ...

Bu nedenle: $\bigcap_{i \in Z^+} A_i = \varnothing$; ve $\bigcup_{i \in Z^+} A_i = \{1,2,3,.....,\} = \mathbf{Z}^+$ dir.

Kuvvet Kümesi

Verilen bir A kümesinin bütün alt kümelerinin kümesine A'nın kuvvet kümesi denir ve P(A) ile gösterilir. $P(A) = \{B : B \subseteq A\}$ dir

Örnek 1.23 : A={ a,b } ise P(A)= { ∅,{a},{b},{a,b}} dir.

Örnek 1.24 : A herhangi bir küme olsun ve kümelerin sırası A, P(A), P(P(A)), P(P(PA))), ... dır.

P*(A) bu ailede A'nın tüm elemanlarının kümesinin ailesini temsil eder.

$P^*(A) = \{x: x \in A$ veya $x \subseteq y$ burada , $y \in P^*(A)\}$ dır ve P*(A) sonsuz bir kümedir.

Bir Kümenin Bölmelenmesi

A bir küme olsun. A'nın bölmelenmesi, A'nın boş olmayan alt kümeleri $\{ S_i : i \in I \}$ dir öyleki;

i) $\bigcup_{i \in I} S_i = A$, ve

ii) $S_i \bigcap S_j = \varnothing$ eğer, bütün $i,j \in I$ için $i \neq j$ ise) dir

Örnek 1.25: a={1,2,3,4,5,6} ise A'nın bölmelenmesi {{1},{2,3},{4,5,6}} dır.

Örnek 1.26: her bir α gerçel sayısı için L_α , $(\alpha,0)$ noktasından geçen düşey çizgi üzerindeki noktaların kümesi olsun:

$L_\alpha = \{ (x,y): x = \alpha$ ve y gerçel bir sayıdır$\} = \{(\alpha,y) : y \in \boldsymbol{R}\}$ dir

$\{ L_\alpha : \alpha \in \boldsymbol{R} \}$ kümelerinin ailesi düzlemi bölmeler : L_α çizgileri üzerindeki her bir nokta ve herhangi iki çizgi birbirinden ayrıdır.

1.3.11 Kartezyen Çarpım

Bir kümenin elemanlarının hangi sıra ile listelendiği önemsizdir. Öte yandan bazı durumlarda

sıra çok önemlidir. Örneğin, koordinat geometride (1,2) noktası ile (2,1) noktası faklıdır.

Sıranın önemli olduğu durumlarla başa çıkmak için x ve y objelerinin **sıralı ikili** (x,y)'yi tanımlarız.

(x,y) = (x',y') sadece ve sadece x=x' ve y=y' ise.

Bu tanımla birlikte açıktır ki (x,y) ile (y,x) faklıdır(x=y değilse) ve sıra önemlidir.

Şu an ileriki bölümlerde temel teşkil edecek iki kümenin Kartezyen çarpımı konseptinin tanımlayabilecek durumdayız.

Tanım: X ve Y kümelerinin kartezyen çarpımı X x Y, x X' e y de Y' ye ait olmak üzere tüm (x,y) sıralı ikililerinin kümesidir.

$$X \times Y = \{(x,y): x \in X \text{ ve } y \in Y\}.$$

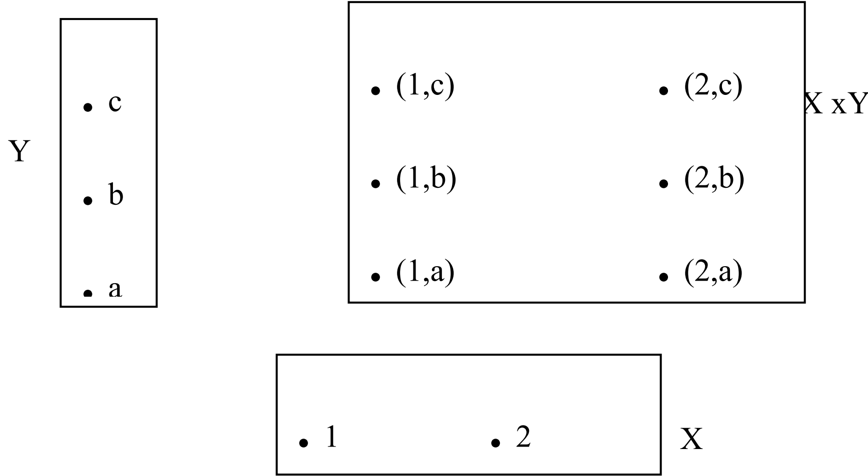
X=Y olması durumunda X x X, X^2 ile gösterilir ve 'X iki' şeklinde okunur, 'X kare' şeklinde değil.

Eğer X veya Y (veya her ikisi de) boş küme ise X x Y de boş kümedir. X ve Y' nin her ikisi de boş olmayan kümeler ise sadece ve sadece X=Y ise X x Y= Y x X 'dir.

Örnek 1.27: Eğer X={1,2} ve Y={a,b,c} ise

X x Y = {(1,a), (1,b), (1,c),(2,a),(2,b),(2,c)}.

X, Y ve X x Y' nin elemanları basit bir Venn şeması ile sistematik olarak gösterilebilir. Bu Venn şeması Şekil 1.3' teki gibidir.



Şekil 1.3

Şekil 1.3 gibi diyagramlar ve R^2= R x R düzleminin koordinat geometri resimleri Kartezyen çarpımının yararlı gösterimleridir. Farklı bir gösterimde ise X ve Y kümeleri Venn diyagramlarındaki gibi iki boyutlu bölgeler yerine tek boyutlu bölgeler olarak çizilir. X ve Y doğru segmentleri olarak çizilir ve elemanları bu doğru segmentinin üzerine yerleştirilir. Uygun olan X'i temsil eden doğrunun yatay olarak çizilmesi ve doğruların birbirine dik olmasıdır. Kartezyen çarpım X 'in üzerinde,Y' nin sağında bulunan dikdörtgensel bölgedir ve (x,y) sıralı ikilileri bu dikdörtgenin içine noktalar dikey olarak x' in üzerine, yatay olarak y' nin sağına gelecek şekilde yerleştirilir.

(x,y) sıralı ikilisi aşağıdaki özellik yardımıyla sıralı n-elemanlı (ordered n-tuple) şekle genelleştirilebilir.

$(x_1,x_2,\ldots,x_n)=(x_1',x_2',\ldots,x_n')$ sadece ve sadece $x_1= x_1'$, $x_2= x_2'$,…, $x_n= x_n'$ ise.

n tane kümenin kartezyen çarpımı iki kümedeki durumun doğal genelleştirilmesidir.

Tanım: X_1, X_2, …, X_n kümelerinin kartezyen çarpımı X_1 x X_2 x …,x X_n ‘dir.

$= \{(x_1,x_2,\ldots,x_n): x_1 \in X_1$ ve $x_2 \in X_2$ ve … ve $x_n \in X_n\}$

$= (x_1,x_2,\ldots,x_n): x_i \in X_i$ i=1,2,…,n olmak üzere}.

Örnek 1.28: A={1,2}, B={a,b} ve C={α , β } ise

A x B x C = {(1,a, α), (1,a, β), (1,b, α), (1,b, β),(2,a, α),(2,a, β),(2,b, α),(2,b, β)}.

Üç kümeden oluşan kartezyen çarpımları göstermek kolay değildir fakat üç boyutlu bölgeler ile gösterilebilecekleri açıktır.

X ve Y sonlu kümeler olmak üzere |X|=n ve |Y|=m ise açıktır ki kartezyen çarpım X x Y, mn elemana sahiptir. Öyle ki;

|X x Y| = |X| **.** |Y|.

Bu sonuç aşağıdaki gibi n tane küme için genelleştirilebilir.

Teorem 1.4: X_1, X_2,…, X_n sonlu kümeler ise | X_1 x X_2 x X_n|=| X_1|**.**| X_2|**.** ….| X_n|.

Kartezyen çarpım işleminin kesişim ve birleşim gibi diğer küme teoremi işlemleri ile nasıl davranacağına geçmeden önce aşağıdaki örneğe bakalım.

Örnek 1.29: A={a,b,c,d}, X={x,y,z}, Y={y,z,t} olsun. Bu durumda

$X \cap Y$={y,z} olur ve
A x ($X \cap Y$)={(a,y),(a,z),(b,y),(b,z), (c,y),(c,z), (d,y),(d,z)}’dır. Şimdi,
A x X={(a,x),(a,y),(a,z), (b,x),(b,y),(b,z),(c,x),(c,y),(c,z), (d,x),(d,y),(d,z)} ve
A x Y={(a,y),(a,z),(a,t), (b,y),(b,z),(b,t),(c,y),(c,z),(c,t), (d,y),(d,z),(d,t)} olur. Bu nedenle,
(A x X) $\cap$(A x Y)={ (a,y),(a,z), (b,y),(b,z), (c,y),(c,z), (d,y),(d,z)} olur.

O halde bu örnekteki kümeler için;

A x ($X \cap Y$)=(A x X) $\cap$(A x Y) olduğuna göre bu özelliğin diğer A, X ve Y kümeleri için de doğru olup olmadığına bakabiliriz.

Aslında yukarıdaki örnekte elde ettiğimiz sonuçlar tüm A, X ve Y kümeler için geçerlidir. Aşağıdaki teoremde Kartezyen çarpımın kesişim ve birleşim işlemlerinde nasıl davrandığını belirten özellikler listelenmiştir.

Teorem 1.5 (i) Tüm A, X ve Y kümeleri için
A x ($X \cap Y$) = (A x X) $\cap$ (A x Y) ve
($X \cap Y$) x A = (X x A)$\cap$ (Y x A). (Bunun anlamı Kartezyen çarpım kesişim üzerine dağılabilir.)
(ii) Tüm A, X ve Y kümeleri için
A x ($X \cup Y$) = (A x X) $\cup$ (A x Y) ve

$(X \cup Y)$ x A = (X x A) $\cup$ (Y x A). (Bunun anlamı Kartezyen çarpım birleşim üzerine dağılabilir.)

İspat: (i). kısmın ispatı şu şekildedir.

$(a,x) \in Ax(X \cap Y)$ olsun. Kartezyen çarpımın tanımından bunun anlamı $a \in A$ ve $x \in (X \cap Y)$' dır. Bu sonuçla, $x \in X$' tir, öyleyse (a,x) A x X' e aittir; $x \in Y$' tir, öyleyse (a,x) A x Y' e aittir. Bu nedenle, $(a,x) \in (A \text{ x } X) \cap (AxY)$' dir ki bu da A x $(X \cap Y) \subseteq (A \text{ x } X) \cap (A \text{ x } Y)$ olduğunu ispatlar.

Alt küme ilişkisini diğer taraftan ispatlamak için; $(a,x) \in (A \text{ x } X) \cap (A \text{ x } Y)$ olsun.

Bu durumda $(a,x) \in$ (A x X) 'tir öyleyse $a \in A$ ve $x \in X$; ayrıca $(a,x) \in$ (A x Y)'tir öyleyse $a \in A$ ve $x \in Y$' dir. Bu nedenle $a \in A$ ve $x \in (X \cap Y)$' dir ve bunun anlamı (a,x) sıralı ikilisi A x $(X \cap Y)$ kartezyen çarpımına aittir. Bundan dolayı $(A \text{ x } X) \cap (A \text{ x } Y) \subseteq A \text{ x } (X \cap Y)$ olmalıdır.

Şu halde A x $(X \cap Y)$ ve $(A \text{ x } X) \cap (A \text{ x } Y)$ kümelerinin eşit olduğu sonucu sağlanmış olur zira her iki küme de birbirinin alt kümesidir.

Son olarak Kartezyen çarpımın alt küme ilişkilerinde nasıl davranacağına ilişkin bir teorem yazabiliriz.

Teorem 1.6: (i) Tüm A, B ve X kümeleri için $A \subseteq B$,$(A \text{ x } X) \subseteq (B \text{ x } X)$ anlamına gelir.

(ii) Eğer X boş olmayan bir küme ise $(A \text{ x } X) \subseteq (B \text{ x } X)$, $A \subseteq B$ anlamına gelir.

1.4 Bağıntılar ve Fonksiyonlar

Bağıntı notasyonu kümeler gibi çok genel bir notasyondur. Bu konu matematiğin anahtar konularından biridir ve başka birçok konuda da kullanılır. Üç özel tip bağıntı çok önemlidir: fonksiyonlar, eşitlik bağıntıları ve sıra bağıntıları.

1.4.1 Bağıntılar ve Gösterimleri

İkili yüklemler yani "…daha ağırdır" şeklindeki cümleleri önermesel fonksiyona çevirmek için iki tane değişkene ihtiyaç vardır. Örneğin, H '…daha ağırdır' anlamına geliyorsa H(x,y) "x, y' den daha ağırdır" önermesel fonksiyonunu ifade eder. İki değişkenli önermesel fonksiyonları iki değişkeni arasındaki ilişkiyi tanımlamak gibi düşünebiliriz. a ve b objeleri verilmiş ise, H(a,b) sadece ve sadece objeleri uygun biçimde ilişkilendirilmiş ise doğrudur.

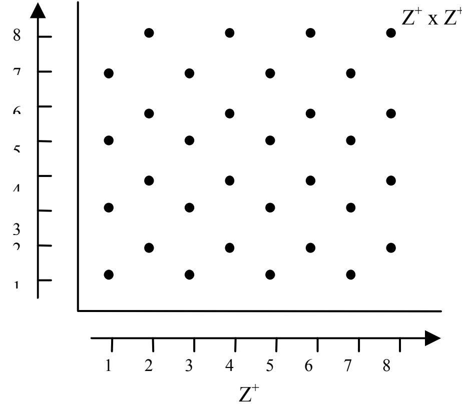
Hatırlanması gereken ilk şey, iki değişkenli önermesel fonksiyon F(x,y)'de değişkenlerin sırasının önemli olduğudur. Özel a ve b objeleri için F(a,b) ile F(b,a) farklı doğruluk değerine sahip olabilir. Önemli olan bir başka şey de x ve y değişkenlerinin farklı tip objeler olabileceğidir. Örneğin, C(x,y) önermesel fonksiyonunu düşünelim: x, y'nin başkentidir. Burada x bir şehir ismi fakat y bir ülke ismidir. O halde, C(a,b)'yi sağlayan (a,b) sıralı ikililerinin kümesi, A={şehirler} B={ülkeler} olmak üzere A x B kartezyen çarpımının alt kümesidir.

Aşağıdaki bağıntı tanımı şaşırtıcı şekilde basit ve geneldir. Bazıları buna ikili bağıntı da der çünkü iki objeyi ilişkilendirir.

Tanım: A ve B iki küme olsun. A'dan B 'ye bir bağıntı A x B kartezyen çarpımının bir alt kümesidir.

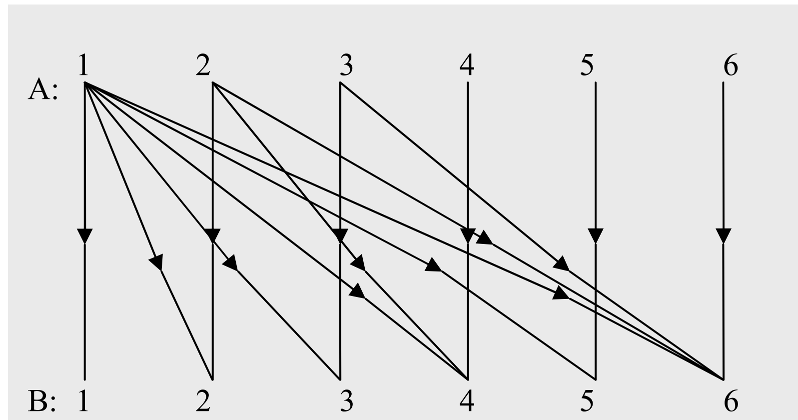
Tanıma bakıldığında ilk göze çarpan bağıntının bir küme olduğudur(sıralı ikililerden oluşan bir küme). ***R***, A'dan B'ye bir bağıntı ise eğer (a,b) ∈***R*** ise a∈A, b∈B ile ilişkilidir deriz. Bu sebeple, ***R*** bağıntısının kendisi basitçe tüm ilişkili eleman çiftlerinin kümesidir. Genellikle kullanılan notasyon 'a, b ile ilişkilidir' için a ***R*** b' dir.

Bağıntıları görsel olarak ifade etmenin çeşitli yolları vardır, özellikle sonlu kümeler arasındaki bağıntıları. Şekil 1.4'de ***R***'nin elemanları A x B kartezyen çarpımının koordinat çizelgesi diyagramı üzerinde işaretlenmiştir. Bu tip diyagramlar ***R***'nin A x B'nin alt kümesi olduğunu açıkça gösterir fakat bağıntının diğer özelliklerini göstermede iyi değillerdir.



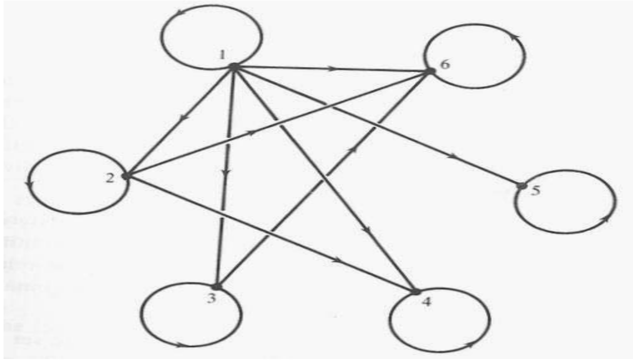
Şekil 1.4

Sonlu kümeler için başka bir alternatif A ve B' nin elemanlarını üst üste yatay şekilde sıralamak ve a ***R*** b olduğunda a∈A' dan b∈B 'ye bir ok çizmektir. Şekil 1.5' de bu çeşit bir diyagram gösterilmiştir.



Şekil 1.5 : Bağıntının diyagram olarak gösterilimi

Şekil 1.5'deki gösterim büyük kümeler için karmaşık hale gelebilir. Öte yandan bir küme üzerindeki bağıntılarda (yani A=B olanlarda), şekil daha basitleştirilebilir. A'daki elemanları iki kere listelemek yerine bu elemanları düzlemde birer nokta olarak temsil edebiliriz. Aynı şekilde a'dan b'ye yönlü bir ok sadece ve sadece a ***R*** b olması durumunda çizilir. Sonuçta ortaya çıkan diyagrama (şekil 1.6) **digraph** denir.



$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Şekil 1.6 : Digraf gösterilimi

Matris göst.

Diğer üçüncü bir bağıntı gösterim biçimi de ikili matristir. A={a_1, $a_{2,\ldots}a_{n,}$} ve B={b_1, $b_{2,}$ … b_m} sonlu kümeler ve R, A'dan B'ye bağıntı olsun. R'nin ikili matrisi n satırlı ve m sütunlu 0 ve 1'lerden oluşan dizi şeklindedir. Eğer bağıntı matrisi elemanları M_{ij} ile gösterilirse ;

Eğer $(a_i,b_j) \in$ R ise M_{ij} =1

$(a_i,b_j) \notin$R ise M_{ij} =0 olarak değer alır.

1.4.2 Bağıntıların Özellikleri

Bağıntıların önemi, ek özellikleri sağlayan özel bir takım bağıntılar yüzündendir. Bu özel bağıntıların ikisi eşlik bağıntıları ve sıra bağıntılarıdır ki bunların ikisi de kümeler üzerindeki bağıntılardır.

Tanım: ***R***, A kümesi üzerinde bir bağıntı olsun. O halde ***R***;

(i) Tüm a $\in$ A için, sadece ve sadece a ***R*** a ise **yansıyandır.** (reflexive).

(ii) Tüm a,b $\in$ A için, sadece ve sadece a ***R*** b, b ***R*** a anlamına geliyorsa **simetriktir.**

(iii) Tüm a,b $\in$ A için sadece ve sadece a ***R*** b ve b ***R*** a, a=b anlamına geliyorsa **ters simetriktir.**

(iv) Tüm a,b,c $\in$ A için sadece ve sadece a ***R*** b ve b ***R*** c, a ***R*** c anlamına geliyorsa **geçişlidir**(transitive).

Örnek 1.30: A={a,b,c,d} ve ***R***={(a,a),(a,b),(a,c),(b,a),(b,b),(b,c),(b,d),(d,d)} olsun.

R bağıntısı yukarıdaki tanımdaki hiçbir özelliği sağlamaz.

R yansıyan değildir çünkü c ***R*** c değildir; bu nedenle tüm x $\in$ A için x ***R*** x doğru değildir.

R simetrik değildir zira örneğin a ***R*** c'dir fakat c ***R*** a değildir.

R ters simetrik değildir zira a ***R*** b ve b ***R*** a 'dır fakat a=b değildir.

R geçişli değildir çünkü a ***R*** b ve b ***R*** d 'dir fakat a ***R*** d değildir.

Verilen digraphlar veya ikili matrisler ile bağıntı özelliklerinin anlaşılması mümkündür. Eğer bağıntı yansıyan bağıntı ise ***R***' nin digraphının her noktasından kendisine bir yönlü ok vardır. İkili matrisinde ise köşegen üzerindeki elemanların hepsi 1' dir.

Eğer ***R*** simetrik ise digraphtaki okların tamamı iki-yönlüdür. Ters simetrik ise okların hiçbiri iki yönlü değildir. Öte yandan geçişli bağıntıların digraphlarından veya ikili matrislerinden özellik tanımlamak zordur.

1.4.3 Kesişimler ve Bağıntıların Birleşimi

A ve B arasındaki ***R*** bağıntısı A x B kartezyen çarpımının alt kümesi olduğuna göre bağıntıların kesişim ve birleşimini tanımlayabiliriz.

R ve ***S***, A kümesinden B kümesine iki bağıntı olsun. Hem $\boldsymbol{R} \cap \boldsymbol{S}$ hem de $\boldsymbol{R} \cup \boldsymbol{S}$ A x B 'nin alt kümesidir. O halde, A'dan B'ye iki bağıntının hem kesişimi hem de birleşimi de aynı zamanda A'dan B'ye bağıntılardır.

R ve ***S*** bağıntılarının farklı küme çiftleri arasında olması durumu ise biraz daha karışıktır. ***R***'nin A'dan B'ye; ***S***'nin ise C'den D'ye bağıntı olduğunu düşünelim. ***R*** ve ***S*** sıralı ikililerden oluşan kümeler olduğundan $\boldsymbol{R} \cap \boldsymbol{S}$ ve $\boldsymbol{R} \cup \boldsymbol{S}$ birer bağıntıdır fakat hangi kümelerin $\boldsymbol{R} \cap \boldsymbol{S}$ ile hangilerinin $\boldsymbol{R} \cup \boldsymbol{S}$ ile ilişkili olduğu çok açık değildir.

Doğal olarak burada, ***R*** ve ***S***, A'dan B'ye bağıntı olduğuna göre kesişim veya birleşimleri bu bağıntıların özelliklerini miras alır mı sorusu akla gelir. Bağıntıların dört özelliğine, ***R*** ve ***S***'nin aynı A kümesi üzerinde bağıntılar olduğunu varsayarak bakalım:

Yansıma özelliğine bakarsak: Hem ***R*** hem de ***S*** yansıyan ise tüm $a \in$ A için $(a,a) \in \boldsymbol{R}$ ve $(a,a) \in \boldsymbol{S}$ olmalıdır. Bu nedenle, (a,a) tüm $a \in$ A için $\boldsymbol{R} \cap \boldsymbol{S}$ ve $\boldsymbol{R} \cup \boldsymbol{S}$'ye aittir, öyleyse ***R*** ve ***S*** 'nin kesişimi ve birleşimi de yansıyandır.

İkinci olarak ***R*** ve ***S***'nin simetrik olduğunu düşünelim. $a,b \in$ A öyle ki $(a,b) \in \boldsymbol{R} \cap \boldsymbol{S}$ olsun. O halde, a ***R*** b ve a ***S*** b' dir. ***R*** ve ***S*** simetrik olduğundan b ***R*** a ve b ***S*** a ' dır ve bunun anlamı da $(b,a) \in \boldsymbol{R} \cap \boldsymbol{S}$' dir. O halde $\boldsymbol{R} \cap \boldsymbol{S}$ de simetriktir. Aynı durum $\boldsymbol{R} \cup \boldsymbol{S}$ için de geçerlidir.

Anti-simetriklik durumu biraz daha karmaşıktır. $\boldsymbol{R} \cap \boldsymbol{S}$ 'nin ters simetrik olduğu yukarıdaki argümanlar ile gösterilebilir fakat birleşim her zaman ters simetrik olmayabilir. Tersine örnekle bunu gösterebiliriz. A={a,b} ve ***R***={(a,b)} ve ***S***={(b,a)}olsun. ***R*** ve ***S*** bağıntıları ters simetrik olduğu açıktır. Fakat $\boldsymbol{R} \cup \boldsymbol{S}$={(a,b), (b,a)}ters simetrik değildir çünkü a b ile, b de a ile ilişkilidir fakat a ve b eşit değildir.

Geçişlilik durumu ise ters simetriye benzer. Geçişli iki bağıntının kesişimi de geçişlidir. Ancak birleşimi geçişli olmayabilir. Aşağıdaki teorem bu özellikleri özetlemektedir.

Teorem 1.7: ***R*** ve ***S*** aynı A kümesi üzerinde iki bağıntı olsun.

a. Hem ***R*** hem de ***S*** yansıyan ise $\boldsymbol{R} \cap \boldsymbol{S}$ ve $\boldsymbol{R} \cup \boldsymbol{S}$ de yansıyandır.

b. ***R*** ve ***S*** simetrik ise $\boldsymbol{R} \cap \boldsymbol{S}$ ve $\boldsymbol{R} \cup \boldsymbol{S}$ de simetriktir.

c. ***R*** ve ***S*** ters simetrik ise $\boldsymbol{R} \cap \boldsymbol{S}$ de ters simetriktir fakat $\boldsymbol{R} \cup \boldsymbol{S}$ ters simetrik olmayabilir.

d. ***R*** ve ***S*** geçişli ise $\boldsymbol{R} \cap \boldsymbol{S}$ ***d***e geçişlidir fakat $\boldsymbol{R} \cup \boldsymbol{S}$ geçişli olmayabilir.

1.4.4 Eşdeğerlik Bağıntısı ve Bölmelemeler

Yaşayan insanlar kümesi üzerinde x ***R*** y sadece ve sadece x, y ülkesinde yaşıyorsa şeklinde tanımlanan bir bağıntıyı düşünelim. Her insanın sadece bir ülkede yaşadığını varsayarsak bağıntı şu üç özelliği sağlar:

x, x ile aynı ülkede yaşamaktadır, o halde yansıyandır.

x, y ile aynı ülkede yaşıyorsa; y de x ile aynı ülkede yaşıyor demektir, o halde simetriktir.

x, y ile aynı ülkede; z de y ile aynı ülkede yaşıyorsa x, z ile aynı ülkede yaşıyor demektir, o halde ***R*** geçişlidir.

Tanım: A kümesi üzerindeki ***R*** bağıntısı yansıyan, simetrik ve geçişli ise bu bağıntı **eşdeğerlik bağıntısı**dır.

Örnek 1.31: A= R (reel sayılar kümesi) olsun ve A üzerinde

x ***R*** y sadece ve sadece $x^2=y^2$ ise

şeklinde bir bağıntı tanımlayalım. O halde;

R yansıyandır zira tüm x reel sayıları için $x^2= x^2$ ‘dir.

R simetriktir zira $x^2=y^2$, $y^2=x^2$ anlamına gelir.

R geçişlidir çünkü $x^2=y^2$ ve $y^2=z^2$ ise $x^2=z^2$ ‘dir.

O halde ***R*** eşdeğerlik bağıntısıdır.

Tanım: ***R***, A kümesi üzerinde bir eşdeğerlik bağıntısı ve $x\in A$ olsun. x’ in **eşdeğerlik sınıfı** [x] ile gösterilir ve A üzerinde x ile ilişkili tüm elemanların kümesidir öyle ki [x]={y∈A: x ***R*** y}.

Eğer iki eleman ilişkili ise eşdeğerlik sınıfları eşittir. Bunu göstermek için diyelim ki ***R***, A üzerinde bir eşdeğerlik bağıntısı ve A’ nın x ve y elemanları için x ***R*** y olsun. [x]=[y] olduğunu göstermek istiyoruz. z∈[x] dersek x ***R*** z olur. x ***R*** y ve ***R*** simetrik ise aynı zamanda y ***R*** x olduğunu biliyoruz. O halde, y ***R*** x ve x ***R*** z ise geçişlilik özelliğinden y ***R*** z yani z∈[y]’ dir. Bu [x] ⊆[y] olduğunu gösterir. [y] ⊆[x] ‘in ispatı da benzer şekilde yapılabilir. Öyleyse, [x]=[y] sonucuna varılabilir.

Teorem 1.8: ***R***, bir A kümesi üzerinde bir eşdeğerlik bağıntısı ve x,y ∈A olsun. Bu durumda sadece ve sadece x ***R*** y ise [x]=[y]’ dir.

Bir küme üzerindeki eşdeğerlik bağıntısının eşdeğerlik sınıfları topluluğu, o kümenin bir bölmelemesini oluşturur.

Teorem 1.9: ***R***, boş olmayan bir A kümesi üzerinde bir eşdeğerlik bağıntısı olsun. Birbirinden farklı R-eşdeğerlik sınıfları topluluğuna A’nın bölmelemesi denir.

Örnek 1.32: ***R***, reel sayılar üzerinde; tamsayı(x) x’ten küçük veya eşit en büyük tamsayı olmak üzere x ***R*** y sadece ve sadece tamsayı(x)=tamsayı(y) ise şeklinde tanımlanmış bir bağıntı olsun.

R’ nin reel sayılar kümesi üzerinde bir eşdeğerlik bağıntısı olduğunu kontrol etmek oldukça basittir. Örneğin; ½ ∈ R: tamsayı(½)=0, öyleyse eşdeğerlik sınıfı

[½] = {x∈ R: tamsayı(x)=0}

= {x∈ R: 0≤x<1}.

Bu kümeye yarı-açık aralık denir ve [0,1) şeklinde ifade edilir.

Bir küme üzerinde verilen eşdeğerlik bağıntısından eşdeğerlik sınıfları ile bölmeleme

tanımlayabileceğimiz gibi bir küme üzerinde verilen bir bölmelemeden de eşdeğerlik sınıfları bölmelemeyi oluşturan orijinal alt kümeler olacak şeklinde bir eşdeğerlik bağıntısı tanımlayabiliriz.

Teorem 1.10: $\{S_i: i\in I\}$ bir A kümesinin bölmelemesi olsun. O halde, $i\in I$ için, x ***R*** y sadece ve sadece $x,y\in S_i$ ise eşdeğerlik sınıfları bölmelemedeki S_i kümeleri olan A üzerinde bir eşdeğerlik bağıntısı tanımlar.

Modulo Aritmetik : n pozitif bir tamsayı olarak verilsin. **Z** tamsayılar kümesi üzerinde ,modulo n bağıntısı aşağıdaki şekilde tanımlanır.

$a\equiv_n b$ ancak ve ancak eğer bazı $k\in\mathbf{Z}$ için a-b = k.n ise

$a\equiv_n b$ için alternatif tanım $a\equiv b \bmod n$ şeklindedir.

Örnek 1.33 : mod5 'de n=5 dir. $a\equiv_5 b$ yi kısa olsun diye a≡ bmod5 şeklinde yazarız. Bu durumda ancak ve ancak a-b =5k ise $a\equiv_5 b$ dir. k gibi bir tamsayı vardır öyleki, a=5k+b dir. Bu yüzden

$[p] =\{q\in\mathbf{Z} : q=5k +p$, bazı $k\in Z$ için$\}$ Eşdeğerlik sınıfları sonsuzdur bazıları:

[0] ={….., -10,-5,0,5,10,15,…..}

[1] ={….., -9,-4,1,6,11,16,…..}

[2] ={….., -8,-3,2,7,12,17,…..}

[3] ={….., -7,-2,3,8,13,18,…..}

[4] ={….., -6,-1,4,7,12,19,…..} Bunlar beş adet farklı eşdeğerlik sınıfıdır.

1.4.5 Bağıntının Kapanışları (Closures of relations)

Bir ülkede farklı şehirlerdeki bilgi işlem merkezleri göz önüne alınırsa bunlar arasında iletişim hattı bulunanların bağıntısı R, (a,b) a ile b arasında bir iletişim var olanları ifade eder. Birbirleri arasında doğrudan iletişim hattı olmayan bu merkezlerin tamamının birbirleriyle haberleşmesinin sağlanması için ilave hat kurulması mümkümüdür? Doğrudan hat bulunmayanlar haberleşemeyeği için bağıntı geçişli olmayacaktır. Böylece tüm çiftler arasında bağlantı olmayacaktır. Eğer tüm merkezlerin birbiri ile haberleşmesini sağlamak istersek en az sayıda bağlantı yaparak bunu gerçekleştirmek nasıl olacaktır. İşte, bulunacak en az sayıda bağlantı ile teşkil edilecek yeni bağıntıya R'nin kapanışı denir. Doğal olarak yansımalı, simetrik ve geçişli bağıntı özelliğine göre kapanışlar da yansıma, simetrik ve geçiş özelliğine sahip olacaklardır.

Tanım: Bir *R* bağıntısının P özelliğine göre kapanışı(closure), R bağıntısının P özelliğini kazanması için en az sayıda sıralı ikili ekleyerek elde edilir. Bir başka ifade ile, Verilmiş olan bağıntı üzerinde yansıma,simetri ve geçişlilik özellikleri mevcut değilse, bağıntının bu özelliklere sahip olabilmesi için yapılan işlemlere bağıntının kapanışları denir.
R bağıntısının Digraf gösteriliminde,

- Yansıyan kapanışını elde etmek için, düğümlere çevrim eklenir
- Simetrik kapanışını elde etmek için, yaylara, ters yönde yay eklenir
- Geçişli kapsanışının elde etmek için, eğer a'dan b'ye bir yol var ise, a'dan b'ye bir yay eklenir.

Not: Yansıyan ve simetrik kapanışları bulmak kolay, oysa geçişli kapanışı bulmak karmaşıktır.

Yansıyan Kapanış :

Tanım: A bir küme ve $\Delta=\{<x, x> \mid x \in A\}$ verilsin. Δ'ya A üzerinde köşegen bağıntı(veya

eşitlik bağıntısı) denir. Δ, A üzerinde yasıma özelliği olan en küçük bağıntıdır(En az sayıda sıralı ikili içerir)

Teorem 1.11:A kümesi üzerinde bir R bağıntısı verilmiş olsun. R'nin yansıyan kapanışı, r(R) = $R \cup \Delta$ 'dır.

- R'nin digraf gösteriliminde tüm düğümlere bir çevrim eklenir
- R'nin bağlantı matrisinin köşegenine 1 koyularak elde edilir.

Örnek1.20: ***Z*** Tamsayılar kümesi üzerinde tanımlanmış olan $R=\{(a,b) \mid a<b\}$ bağıntısının yansıyan kapanışı nedir?

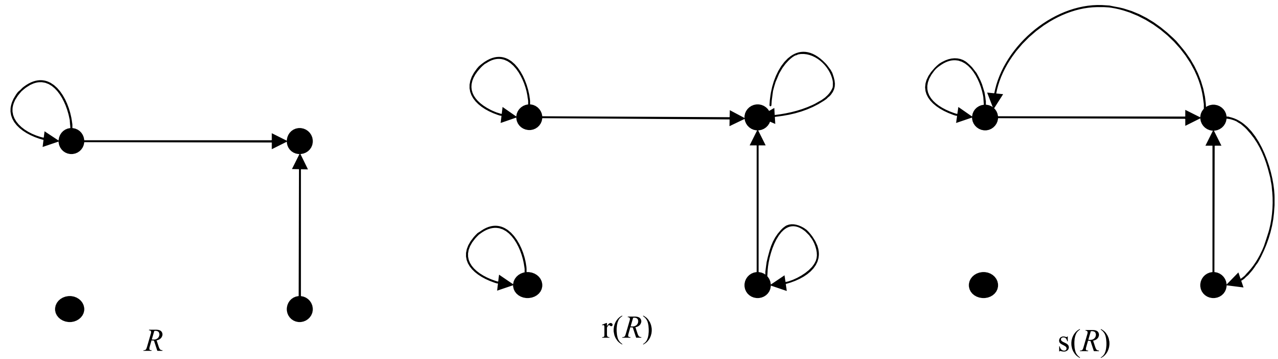
Çözüm: R'nin yansıyan kapanışı :
$r(R) = R \cup \Delta = \{(a,b) \mid a<b\} \cup \{(a,a) \mid a \in \boldsymbol{Z}\} = \{(a,b) \mid a \leq b\}$ dir.

Simetrik Kapanış
Tanım: A kümesi üzerinde bir R bağıntısı verilmiş olsun R^{-1} veya R'nin tersi $R^{-1} = \{< y,x > \mid < x,y > \in R\}$ bağıntısıdır.
R^{-1} 'i bulmak için;

- R'nin digraf gösteriliminde tüm yayların tersini al
- R'nin bağlantı matrisi M 'nin M^T transpozunu al.

Bu bağıntı R^T veya R^c olarak gösterilir ve R 'nin tersi denir.

Teorem 1.12.: A kümesi üzerinde bir R bağıntısı verilmiş olsun. R'nin simetrik kapanışı, s(R) = $R \cup R^{-1}$ dir.
Örnek 1.34.: ***Z*** Tamsayılar kümesi üzerinde tanımlanmış olan $R=\{(a,b) \mid a>b\}$ bağıntısının simetrik kapanışı nedir?
Çözüm. R'nin simetrik kapanışı :
$s(R) = R \cup R^{-1} = \{(a,b) \mid a>b\} \cup \{(b,a) \mid a>b\} = \{(a,b) \mid a \neq b\}$ dir.
Bu son eşitlikte R, birincisi ikincisinden büyük olan sıralı pozitif tamsayı çiftini, R^{-1} ise birincisi ikincisinden küçük olan sıralı pozitif tamsayı çiftini temsil eder.



Şekil 1.7. yansıyan ve simetrik kapanış örneği

Örnekler:
• Eğer $A = Z$ ise $r(\neq) = Z \times Z$ *dir.*
• Eğer $A = Z^+$ise, $s(<) = \neq$) dir.

s(<) 'ın bağlantı matrisi nasıl olur??

• Eğer $A = Z$, ise s(≤) = ?

Teorem 1.13: R_1 ve R_2, A'dan B'ye verilmiş bağıntılar olsun Bağıntılar aşağıdaki özellikleri sağlar.
• $(R^{-1})^{-1} = R$
• $(R_1 \cup R_2)^{-1} = R_1^{-1} \cup R_2^{-1}$
• $(R_1 \cap R_2) -1 = R_1^{-1} \cap R_2^{-1}$
• $(A \times B)^{-1} = B \times A$
• $\varnothing^{-1} = \varnothing$
• $\overline{R}^{-1} = \overline{R^{-1}}$
• $(R_1 - R_2)^{-1} = R_1^{-1} - R_2^{-1}$
• Eğer $A = B$, ise $(R_1R_2)^{-1} = R_2^{-1} R_1^{-1}$ *dir.*
• Eğer $R_1 \subseteq R_2$ ise, $R_1^{-1} \subseteq R_2^{-1}$

Teorem 1.14.: Ancak ve ancak R simetrik ise, $R = R^{-1}$ *dir.*

Yollar(Dolaşılar)
Tanım: Yol, kenarlar üzerinde giderek oluşturulan bir yönlü graftır.
Bir yönlü G grafında a'dan b'ye yol uzunluğu n $<x_0, x_1><x_1, x_2> \ldots <x_{n-1}, x_n>$olan kenarların dizisidir. Önceki kenarın bitiş düğümü, sonraki kenarın başlangıç düğümü ile çakışmalıdır.
Eğer $x_0 = x_n$ ise, devre veya devir olarak adlandırılır.
Benzer olarak bağıntılar için;

Teorem 1.15.: A üzerinde bir R bağıntısı verilsin.Ancak ve ancak, $<a, b> \in R^n$ ise, a'dan b'ye uzunluğu n olan bir yol vardır.
İspat: (Tümevarın ile)
Temel adım. a'dan b'ye, 1 uzunluğundaki yolda $R^1=R$ dir. Buradan iddia n=1 için doğrudur.
Tümevarım hipotezi: İddia'nın n için doğru olduğunu kabul edelim ve n+1 için de doğruluğunu ispatlayalım.
Ancak ve ancak , A'da, a'dan x'e 1 uzunluğunda yolu olan bir x var ve x'ten b'ye n uzunluğunda bir yol var ise a'dan b'ye n+1 uzunluğunda bir yol vardır.

Tümevarım hipotezinden,
$<a, x> \in R$ ve <x,b> n uzunluğunda bir yol olduğundan $<x, b> \in R^n$ dir.
Eğer $<a, x> \in R$ *ve* $<x, b> \in R^n$ ise $<a, b> \in R^n.R = R^{n+1}$ dir.
Teorem: A'daki bir R bağıntısı,ancak ve ancak $R^n \subseteq R$ ise geçişlidir.(n=1,2,3,…..)
Geçişli Kapanış
Bir bağıntının geçişli kapanışının bulunması için yönlü graftaki hangi düğüm çiftlerinin birbirine bağlanacağının bulunması gereklidir.
Tanım: A kümesi üzerinde bir R bağıntısı verilsin. R^* bağlılık bağıntısı R'deki a ve b arasında bir yol olan (a,b) leri içerir. Örnekler:
• $A = Z$ ve $R = \{<i, i+1>\}$ *ise* ,$R^* = <$.
• A = insanlar kümesi, ve $R = \{<x, y> \mid$ x, y'nin ebeveyni ise$\}$. R^* = *nedir*?

R^n , a'dan b'ye uzunluğu n olan yollara sahip (a,b) çiftini içerdiği için, R^* , tüm R^n'lerin birleşimidir. Başka bir ifade ile,

$$R^* = \bigcup_{n=1}^{\infty} R^n \text{ dir.}$$

Örnek1.22: İstanbul'daki otobüs durakları arasında otobüs değiştirmeden gidilebilen (a,b) durak çiftlerinin bağıntısı R olarak verilsin. N pozitif tamsayı ise R^* nedir? R^n nedir?

Çözüm: R^n , a durağından b durağına gitmek için en fazla n-1 otobüs değiştirilen (a,b)'leri içerir. R^*, ise a'dan b'ye gitmek için daha fazla otobüs değiştirmeyi gerektiren(a,b) sıralı çiftlerini içerir.

Tanım: Bir *R* bağıntısının t(*R*) geçişli kapanışı, *R*'yi içeren en küçük geçişli bağıntıdır. Buradan, eğer a'dan b'ye bir yol var ise, a'dan b'ye bir yay olmalıdır. Veya (a,b,) $\in R$ dir.

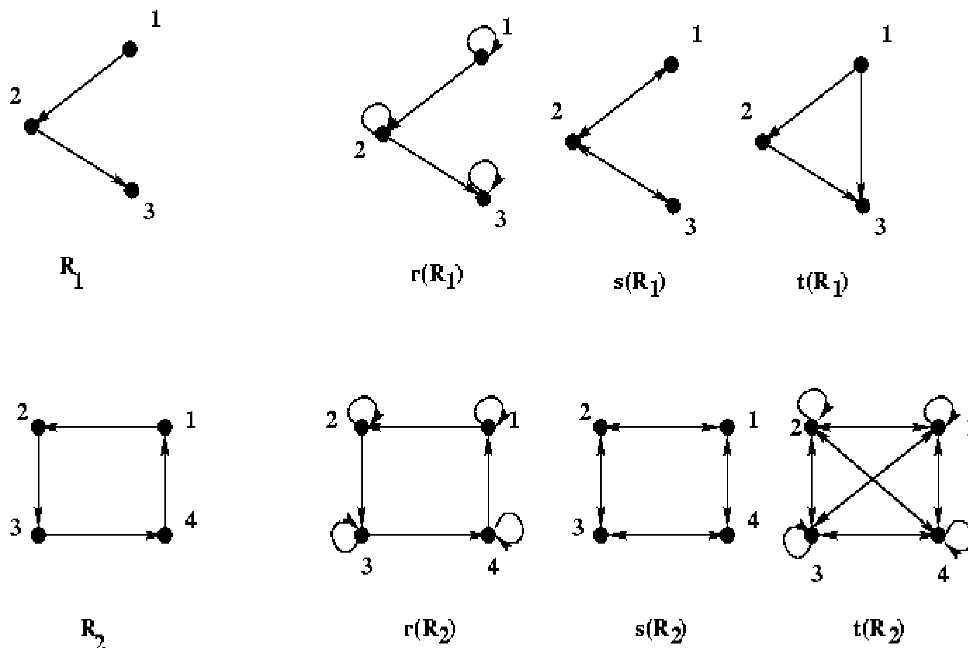
Örnek:
• Eğer $A = Z$ ve $R = \{< i, i+1>\}$ ise $t(R) = <$

Teorem 1.16.: $t(R) = R^*$.dir.
İspat için R^*'ın
1) geçişli bir bağıntı olduğunu,
2) *R* 'yi içerdiğini
3) *R*'yi içeren en küçük geçişli bağıntı olduğunu göstermek gereklidir.

İspat:

2. kısmın ispatı R^*'ın tanımından kolaydır $R^* = \bigcup_{n=1}^{\infty} R^n$ $R \subseteq R^*$ dır. O halde R^*' *R*'yi içerir

1. kısmın ispat.
Eğer (a,b) $\in R^*$ *ve* (b,c)$\in R^*$ ise, R^*'ın tanımından R^m'de a'dan b'ye ve R^n*'de* b'den c'ye bir yol vardır. Bu durumda a'dan c'ye b'yi takip ederek R^* 'ın içerdiği $R^m R^n = R^{m+n}$ de bir yol bulunabilir. Öyleyse (a,c)$\in R^*$ dir. Bu sonuç R^*'ın geçişli olduğunu gösterir.
3. kısmın ipatı:
S'nin *R*'yi içeren herhangi bir geçişli bağıntı olduğunu kabul edelim. R^*'ın en küçük bağıntı olduğunu göstermek için *S*'nin R^*'ı içerdiğini göstermeliyiz.
$R \subset S$ dir. Böylece, *S* geçişli olduğundan $R^2 \subset S^2 \subset S$ dir.
Bu nedenle, bütün n'ler için $R^n \subset S^n \subset S$ dir(geçişli bağıntılar için teorem). Buradan *S*, *R*'nin tüm üslerinin bileşimini içerdiği için R^*'ıda içerir.



Şekil 1.8. yansıyan, simetrik ve geçişli kapanış için örnekler

Teorem 1.17.: Eğer $|A| = n$, ise uzunluğu n'den büyük olan bir yol bir çevrim içerir.
ispat:

Eğer, R bağıntısının n ayrıtlı digraf gösteriliminden n'den fazla ayrıt içeren bir liste tanımlanırsa burada aynı ayrıt en az iki kere geçmelidir.(eğer, k adet kutuya k+1 ve daha fazla nesne yerleştirilirse, en az bir kutuya birden fazla nesne yerleşmelidir. Pigeon Hole prensibi).

Böylece, $k > n$ için R^k 'da R'nin ilk n kuvvetinde olmayan bir yay bulunmaz.

Sonuç: Eğer | A | = n, ise $t(R) = R^* = R \cup R^2 \cup \ldots \cup R^n$ dir
Sonuç: t(R) 'nin bağlantı matrisini, R'nin bağlantı matrisinin ilk n kuvvetinin bileşimi olarak hesaplayabiliriz.

R*'ı bulmak için algoritma

- R^* 'ın tanımının doğrudan uygulaması(n eleman ve M matrisi verilen bir bağıntı)

- $C = M$, $T = M$.
- for i=2 to n
  - $T = M \otimes T$ hesapla(mantıksal çarpım; bu Mi olacak)
  - $C = C \vee T$ hesapla (öncekilerle bileşimini al)

Karmaşıklık hesabı

- Çevrim $n - 1$ kez yapılır
- Her defada, Mantıksal VEYA (O(n^2) kere) ve bir matris çarpımı (O(n^3) kere)
- Toplam zaman: O(n^4) dür

Hızlandırma işlemleri

- Hızlı Matris çarpımı
  - Strassen – O(*n*log27) ≈ O(*n*2.81)
  - Leading to O(*n*3.81)
- Hızlı mantıksal matris çarpımı
  - Four Russians algorithm – O(*n*4/log2*n*)
- VE ve VEYA'lar ile farklı bir formül ile hesaplama
  - Warshall's algorithm – O(*n*3))

Kapanışların Özellikleri

Bir A kümesi üzerinde verilen R bağıntısı $R^{-1} = \{ (a, b) \mid (b, a) \in R\}$ aşağıdaki özelliklere sahiptir.

$r(R) = R \cup \Delta \quad (\Delta = \{\langle x, x\rangle \mid x \in A\})$

$s(R) = R \cup R^{-1}$

3. $t(R) = \bigcup_{i=1}^{\infty} R^i = \bigcup_{i=1}^{n} R^i$ Eğer |A| = n.

4. Ancak ve ancak, r(R) = R ise R yansıyandır.

5. Ancak ve ancak, s(R) = R ise R simetriktir.

6. Ancak ve ancak, $t(R) = R$ *ise* R geçişlidir.

1.4.6 n-ögeli(n-tuple) bağıntılar ve uygulamaları

Birden fazla küme arasındaki bağıntılar sık sık karşımıza çıkar. Örneğin, öğrenci adı, öğrencinin bölümü, öğrencinin başarı notunu içeren kümeler arasında bir bağıntı vardır. Bu bölümde birden fazla kümeler arasında olan ve n-ögeli(n-tuple) bağıntılar olarak adlandırılan bağıntılar açıklanacaktır.

Tanım: A_1, A_2, ,……, A_n: kümesi verilsin. Bu kümeler üzerindeki bir n-ögeli bağıntı, $A_1XA_2X……XA_n$ kartezyen çarpımının bir alt kümesidir. A_1, A_2, ,……, A_n kümelerine bağıntının alanı(domain) ve n'e derecesi denir.

Örnek 1.35: 5 ögeli(B, N, A, D,N) bir R bağıntısı B: Bölümü, N :Numarası, A: Öğrencini adı, D : Dersin adı, N: Notu 'nu göstermek üzere veriliyor. Örneğin, Bilgisayar mühendisliği bölümü 01104115 numaralı Ali nin Ayrık Matematik dersi notu BA'nın anlamı (Bilgisayar,01104115, Ahmet, Ayrık matematik,BA) R bağıntısına aittir. Bu durumda derecesi 5 olan R bağıntısının alanı olan kümeler, Bölümler,Öğrenci numaraları, Öğrenci adları, Dersler ve Notlar şeklinde olacaktır.

Uygulama: İlişkisel Veritabanları

Bilgiyi saklamak ve işlemek için tasarlanmış bilgisayar sistemine veritabanı sistemi denir. Saklanmış verilerin işlenmesinin kontrol eden yazılıma da veritabanı yönetim sistemi (database management system) veya DBMS denir.

Tüm veritabanı yönetim sistemleri, verinin özel bir tip yapıya sahip olduğunu ve DBMS' in saklı veriyi, verinin kendi teorik modeline göre işlediğini varsayar. Bu yüzden birçok değişik tip DBMS bulunur: ilişkisel, ağ ve hiyerarşik. Bu bölümde matematiksel bağıntıları esas alan ilişkisel veritabanı sistemlerinden bahsedilecektir.

Bir veri birçok kısımdan oluşur. Örneğin, adres defterindeki bir kayıt isime, adrese, telefon numarasına göre sınıflandırılabilir. Verinin her bir parçası 'attribute (nitelik)' olarak adlandırılır. Verilerin her zaman belli bir nitelik kümesine sahip olduğunu varsayarız ve bu nitelik kümesine kayıt tipi(record type) adı verilir. Bir kayıt dosyası (record file), verilen kayıt tipine ait verilerin toplamıdır. Tüm verilerin aynı tip olduğu kayıt dosyalarına **birincil normal form**dadır **(first normal form**) denir. İlişkisel veritabanlarının temel kuralı tüm kayıt dosyalarının birincil normal formda olmasıdır.

Tanım: Veri **attribute** adı denilen bileşenlerine ayrılır. Bir **kayıt tipi** bir attributelar(veya **field**lar) kümesidir. Bir **kayıt örneği** (record instance), belli bir kayıt tipinin gerçek verisidir ve **kayıt dosyası** aynı kayıt tipinden olan kayıt örneklerinin kümesidir.

Örnek 1.36: GYTE isimli bir yardım derneği kendisine yapılan bağışları yapan kişileri, isimlerini, adreslerini, telefon numaralarını ve bağışla ilgili diğer detayların bilgilerini tutmak istediğini varsayalım.

Öncelikle bu dernek; bağışlayanın_adı, bağışlayanın_adresi, bağışlayanın_telefonu, bağış_miktarı ve bağış_tarihi şeklinde adlandırabileceğimiz attribute' ları belirler. Bu beş attribute kayıt tipini tanımlar. Tablo 1.1' de bazı kayıt örnekleri gösterilmiştir.

bağışlayanı_adı	*bağışlayanın_adresi*	*bağışlayanın_telefonu*	*bağış_miktarı*	*bağış_tarihi*
Kaya, R	Çayırova, Kocaeli	262 614-3939	100	Ocak 1997
Kaya, R	Çayırova, Kocaeli	262 614-3939	150	Mart 1999
Beyaz, S	Gebze, Kocaeli	262 578-4108	300	Ekim 1998
Verir,S	Pendik,İstanbul	216 467-1297	250	Kasım 2000
Verir, S	Pendik,İstanbul	216 467-1297	500	Aralık 1999

Tablo 1.1

Bağış yapanın açık adresi sadece bir attribute ile etiketlendiğinden bu kayıt dosyasından coğrafik bilgiyi elde etmek kolay olmayabilir. Örneğin dernek, İstanbul'dan bağış yapanları bulmak isterse şehir adı tek başına bir attribute olarak istenmediğinden çok zor olacaktır. bağışlayanın_adresi isimli tek bir attribute cadde ve şehir olarak ikiye ayrılsaydı şirketin işi çok daha kolay olurdu.

Bu örnek, attribute tanımlamak için önemli bir noktayı göstermiştir. Bir kayıt örneğindeki potansiyel yararlı bilgi parçalarının her biri bir attribute ile belirtilmelidir. Bu mecburi bir kural değildir zira 'potansiyel yararlı bilgi parçası' verinin kullanıldığı yere göre değişir. Yukarıdaki örnekte eğer coğrafik konumun bir önemi yoksa adresleri tek bir attribute olarak belirtmek daha mantıklıdır.

İlişkisel veritabanı modelinde kayıt dosyası bir tablo olarak gösterilir. Tablonun sütunları attribute isimlerini, satırları ise her bir kayıt örneğini oluşturur.

Bir kayıt tipinin A_1, A_2,…,A_n şeklinde n tane attribute' tan oluştuğunu düşünelim. Bu durumda herhangi bir A_i attribute' u için bir veri girişleri kümesi olacaktır. X_i' ye de A_i attribute' u ile elde edilen değerler kümesi diyelim. X_i kümeleri zamana bağımlıdır ve kayıt dosyasına yeni girişler oldukça veya kayıt silindikçe değişir.

Bu notasyona göre; verilen bir kayıt örneği her bir x_i, Xi kümesine ait olmak üzere n-tuple' dır(x_1, x_2,…x_n). Bunun anlamı tüm kayıt örnekleri n tane aynı tip bilgi parçasından oluşur. $x_i \in X_i$ olmak üzere tüm n-tuple' ların (x_1, x_2,…x_n) kümesi X_1 x X_2 x…x X_n kartezyen çarpımıdır. Bu yüzden R kayıt dosyası kartezyen çarpımın alt kümesidir ($R \subseteq (X_1 \times X_2 \times \ldots \times X_n)$).

Örnek 1.37: A_1…A_5 sırasıyla bağışlayanın_adı, bağışlayanın_adresi, bağışlayanın_telefonu, bağış_miktarı ve bağış_tarihi olsun. Her bir A_i attribute' u için bu attribute'a karşılık gelen X_i kümesi olduğunu varsayarız. O halde, bir kayıt örneği $x_i \in X_i$ olmak üzere 5 ögeli (5-tuple)' dır.

Bu kayıt tipine göre önemli sayıda bilgi yinelemesi olur. Örneğin, bağış yapanın ismi, adresi ve telefonu her bağış yaptığında tekrar kaydedilir. Bu bilginin tutulduğu yerden kayıplara yol açacağı gibi kayıt dosyasının güncellenmesini de zorlaştırır. Mesela, iki bağış yapmış Bay Kaya adres değiştirdi diyelim. Bu durumda, kayıt dosyasını güncelleştirmek için iki kayıtta da adresi değiştirmek gerekecektir.

Bu sebeplerle veriyi aşağıdaki gibi iki ayrı kayıt dosyasına bölmek daha mantıklıdır.

A_1, A_2, A_3: bağışlayanın_adı, bağışlayanın_adresi, bağışlayanın_telefonu

A_1, A_4, A_5: bağışlayanın_adı, bağış_miktarı, bağış_tarihi

Bu durumda orijinal veritabanındaki yineleme probleminden kurtulmuş oluruz ve daha kolay güncelleme yapabiliriz. Mevcut durumda veritabanı iki ilişkili kayıt dosyası içerir; birisi X_1 x X_2 x X_3 'ün, diğeri X_1 x X_4 x X_5 'ün alt kümesidir. Tabii ki, iki kayıt dosyasını bağışlayanın_adı attribute' u bağlar.

Tablo 1.2 ve tablo 1.3, tablo 1.1' deki bilginin nasıl iki kayıt dosyasına ayrıldığını göstermektedir.

bağışlayanın_adı	***bağışlayanın_adresi***	***bağışlayanın_telefonu***
Kaya, R	Çayırova, Kocaeli	262 614-3939
Verir,S	Pendik,İstanbul	216 467-1297
Beyaz, S	Gebze, Kocaeli	262 578-4108

Tablo 1.2

bağışlayanın_adı	*bağış_miktarı*	*bağış_tarihi*
Kaya, R	100	Ocak 1997
Kaya, R	150	Mart 1999
Beyaz, S	300	Ekim 1998
Verir,S	250	Kasım 2000
Verir, S	500	Aralık 1999

Tablo 1.3

Tanım: A_1, A_2,…, A_n attribute' ler topluluğu olsun ve her bir A_i' ye ilişkin bir X_i veri kümesi olduğunu düşünelim. **İlişkisel veritabanı** her biri bazı X_i kümeleri arasındaki bağıntılar topluluğudur. Her bir bağıntı bir **kayıt dosyası**dır.

Kayıt dosyasındaki kayıt örneklerine anahtar (key) ile erişilir. Key, tek bir kayıt örneğini belirten attribute' lar kümesidir, fakat bu kümenin hiçbir öz alt kümesi tek bir kayıt örneğini belirtme özelliğine sahip değildir.

Pratikte birçok olası anahtar seçme imkânı vardır. Key olarak kullanılabilecek attribute'ler kümesine **candidate key** denir. Bunlardan biri gerçek key olarak seçilir ve buna **primary (birincil) key** denir.

Örneğimizde, {bağışlayanın_adı} herhangi iki bağış yapanın adının aynı olmaması durumunda Tablo 1.3 için bir candidate keydir. Bu durumda her bir kayıt örneği bağış yapanın adı ile belirtilebilir. Öte yandan iki farklı bağış yapan kişinin aynı adı taşıması durumunda {bağışlayanın_adı} key olmaz bunun yerine {bağışlayanın_adı, bağışlayanın_telefonu} attribute kümesi key olarak kullanılabilir.

İlişkisel veritabanları üzerinde beş çeşit işlem yapılabilir.

Selection (Seçme)

Selection işlemi kayıt dosyasından verilen kıstas kümesini sağlayan kayıt örneklerini listeler. Örneğin, X şehrinde yaşayan müşterilerin tüm isim ve adres kayıtlarını listelemek bir selection örneğidir.

Selection işlemini yeni kayıt dosyaları tanımlamak yani veri tabanındaki kayıt dosyalarının alt kümeleri şeklinde düşünebiliriz. Bu yeni kayıt dosyaları muhtemelen geçicidir ve veritabanını oluşturan kayıt dosyaları kümesine eklenmezler. Aynı zamanda selection kayıt dosyasının tablo gösterimi şeklinde de tanımlanabilir. Bu yeni kayıt dosyaları gerekli attribute'lara sahip satırları çekerek elde edilir.

Örneğin; GYTE veritabanında 'Ocak 1999'dan sonraki tüm bağışları seçmek' istediğimizde tablo 1.3 'te gösterilen kayıt dosyasından ikinci, dördüncü ve beşinci satırlar elde edilecektir.

İzdüşüm (Projection)

Selection tablodaki belli satırları geri döndürürken projection işlemi sütunları döndürür. Sütunlar attribute' lara karşılık geldiğinden sonuçta ortaya çıkan kayıt dosyası orijinalden daha az sayıda attributelu kayıt tipine sahiptir.

Projection işleminin resmi tanımı şöyledir: R, (A_1, …, A_p) tipinde bir kayıt dosyası ve $q \leq p$ ve her bir B_i aynı zamanda R' nin attribute' u olmak üzere (B_1,…, B_q) kayıt tipi olsun. Yani, her bir B bir j için A_j' ye eşit olsun. Projection, kayıt örnekleri R' nin her bir kayıt örneklerinin B_i attribute' larından oluşan (B_1, …, B_q) tipinde yeni kayıt dosyası tanımlar. Özet olarak projeksiyon, p ögeli bağıntıyı q ögeliye dönüştürür (Burada $q \leq p$ dir)

Doğal Birleşim (Natural Join)

GYTE veritabanının örnek 1.37 'deki gibi ikiye ayrıldığını düşünelim. Bu durumda bağış yapanların isimlerini, telefon numaralarının ve bağış miktarlarını nasıl alabiliriz? Buradaki problem bağış yapanın telefon numarası ile bağış miktarlarının farklı kayıt dosyalarında olmalarıdır. O halde kayıt dosyalarını birleştirerek üç attribute 'u da içeren yeni bir kayıt dosyası üretmemiz gerekir. İki dosyada ayrıca bağışlayanın_adresi ve bağış_tarihi de bulunur ve sonuçta oluşacak birleşmiş tabloda bu attributeler de bulunacaktır. Ancak bu bir sorun değildir zira projection ile bu dosyadan gerekli kayıt tipleri çekilebilir.

Natural join işleminin matematiksel temeli şöyledir: R ve S, $(A_1,\ldots, A_p, B_1,\ldots, B_q)$ ve $(A_1,\ldots, A_p, C_1,\ldots, C_r)$ tipinde kayıt dosyaları olsun. R ve S' nin doğal birleşimi $(A_1,\ldots, A_p, B_1,\ldots, B_q, C_1,\ldots, C_r)$ tipinde yeni bir kayıt dosyasıdır. Doğal birleşimim oluşturan kayıt örneklerinin hepsi $(x_1,\ldots, x_p, y_1,\ldots y_q) \in R$ ve $(x_1,\ldots, x_p, z_1,\ldots z_r) \in S$ özelliğine sahip (p+q+r)-tuple $(x_1,\ldots, x_p, y_1,\ldots y_q, z_1,\ldots,z_r)$ 'dır.

Birleşim ve Fark (Union and Difference)

Verilen iki aynı kayıt tipinde R ve S kayıt dosyasının birleşimi ve farkı, bildiğimiz küme teorisindeki birleşim ve fark işlemlerine karşılık gelir. Bu yüzden $R \cup S$, ve R ve S 'deki kayıt örneklerinin tamamını (listeyi tekrarlamadan) içeren kayıt dosyasıdır. R-S ise R de bulunan fakat S' de bulunmayan kayıt örneklerini içeren kayıt dosyasıdır.

1.4.7 Sıra Bağıntıları

Birçok küme doğal olarak sıralanmış elemanlara sahiptir. Örneğin büyüklüğe göre sıralanmış reel sayılar kümesi. Benzer şekilde bir küme topluluğu eleman sayısına göre sıralanabilir. Örneğin, $A \subseteq B$ ise A, B' den küçüktür deriz.

Eşdeğerlik bağıntılarından farklı olarak birçok farklı tip sıra bağıntısı vardır. En genel sıra bağıntısı 'parçalı sıra' bağıntısıdır.

A kümesinde bir ***R*** bağıntısı verilmiş olsun. ***R*** bağıntısı;

a:Yansıma ($\forall$ a $\in$ A için, sadece ve sadece a ***R*** a ise **yansıyandır**(reflexive)).

b. Ters Simetrik :($\forall$ a,b $\in$ A için sadece ve sadece a ***R*** b ve b ***R*** a, a=b anlamına geliyorsa **ters simetriktir)**

c. Geçişlilik : ($\forall$ a,b,c $\in$ A için sadece ve sadece a ***R*** b ve b ***R*** c, a ***R*** c anlamına geliyorsa **geçişlidir**(transitive)).

Özelliklerine sahip olsun. Bu özelliği taşıyan kümelere kısmi sıralı kümeler(Partially Ordered Set, POSET) denir.

Tanım: Bir kümedeki **parçalı sıra**, yansıyan, ters simetrik ve geçişli olan bir bağıntıdır.

Bir kümede parçalı sıra varsa bu kümeye **parçalı sıralı küme(POSET)** denir.

Örnek 1.38: Kümelerde alt küme($\subseteq$) bağıntısı ,

Doğal sayılarda bölünebilirlik; $a/b \Rightarrow ak=b$, $a,k,b \in N$; 2/5

Sıralama için ≤ sembolü kullanılır. $a \leq b$; a, b'nin önünde gelir anlamındadır.

Kısmi sırlama denmesinin nedeni küme içinde birbiriyle karşılaştırılamayan elemanlar

olabileceği nedeniyledir.

Örnek 1.39: Reel sayılar kümesi üzerinde x ***R*** y sadece ve sadece $x \leq y$ ise şeklinde tanımlanan ***R*** bağıntısı parçalı sıradır.

Öte yandan, x ***S*** y sadece ve sadece x<y ise şeklinde tanımlanan ***S*** bağıntısı parçalı sıra değildir çünkü yansıyan değildir.

Teorem 1.18: ***R***, A kümesi üzerinde parçalı bir sıra ve B de A'nın herhangi bir alt kümesi olsun. Bu durumda, ***S***=***R***$\cap$(B x B) B üzerinde bir parçalı sıradır.

Topyekûn sıra: (Doğrusal sıra) : Kümenin her hangi iki elemanı arasında sıralama yapılabilirse topyekûn sıra bağıntısı vardır. (Doğal sayılarda büyüklük, küçüklük bağıntısı)

Sözlük sırası : S ve T topyekûn sıralı kümeler ise SXT (kartezyen çarpım) kümesinde sözlük sırası:

a, a'$\in$ S; b, b'$\in$ T olmak üzere;

(a,b) < (a',b') $\Rightarrow$ a < a' yada a=a', b<b' dür.

Örnek: A= (1,2,3,4,6,8,12) kümesinde bölünebilirlik bağıntısıyla kısmi bir sıralama yapılırsa, bağıntı matrisi Tablo 1.4'deki şekilde olacaktır.

	1	2	3	4	6	8	12
1	1	1	1	1	1	1	1
2	0	1	0	1	1	1	1
3	0	0	1	0	1	0	1
4	0	0	0	1	0	1	1
6	0	0	0	0	1	0	1
8	0	0	0	0	0	1	0
12	0	0	0	0	0	0	1

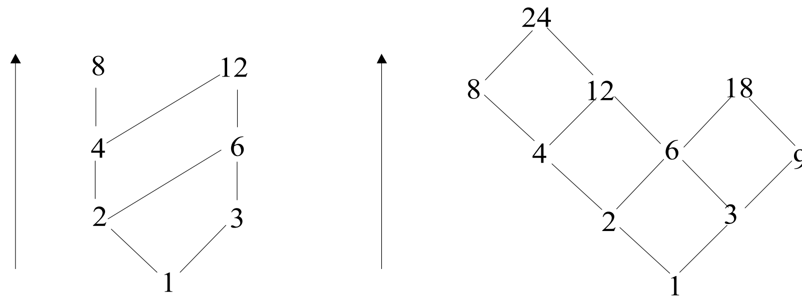
Tablo 1.4.

Halef-Selef(Predecessor-Successor, ilk öndegelen- ilk izleyen) Bağıntısı:

b, a'nın halefi ise a<c<b olamaz. Yani a ile b arasında sırlanabilen bir c elemanı bulmak mümkün değildir, yani a << b'dir.

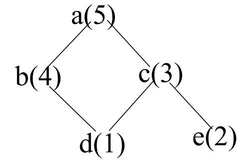
Bu durumda kısmi sıralı küme için yeni bir graf tanımı(hasse diyagramı) yapılarak çizilir.

Hasse Diyagramı: a<<b şeklindeki çiftleri birleştiren ve en önde gelenin en alta konulduğu graftır. Örnek: Şekil 1.9.



Şekil 1.9

Düzgün Sayılama(Consistent Enumeration) :Bu bir fonksiyondur



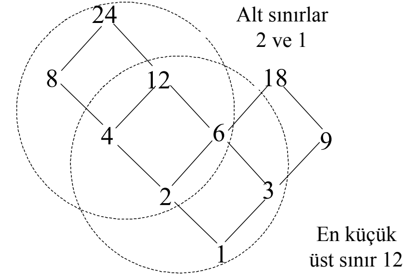
Şekil 1.10.

f**:** $S \rightarrow N$; öyleki $a \leq b \Rightarrow f(a) \leq f(b)$

Parantez içindeki sayıları vererek düzgün sayılama yapılabilir.

Burada; en büyük(maksimal) eleman (a) bir tane (kendinden sonra gelen yok)

en küçük(minimal) eleman (d,e) iki tane(Kendinden önce gelen yok)



Şekil 1.11

Infimum, Supremum

S bir POSET , $A \subseteq S$ alt POSET

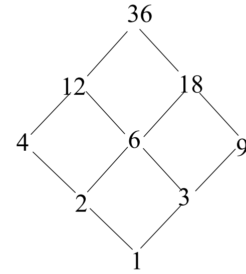
$\forall a \in A$ $m^{\vee} \leq a$ olacak şeklide $m^{\vee}$ mevcut ise $m^{\vee}$ A'nın bir alt sınırıdır.

$\forall a \in A$ $a \leq m^{\wedge}$ olacak şeklide $m^{\wedge}$ mevcut ise $m^{\wedge}$ A'nın bir üst sınırıdır.

Eğer A'nın bir üst sınırı, A'nın diğer bütün üst sınırlarından önde geliyorsa buna A'nın supremumu denir. En küçük üst sınır(Least Upper Bound) = Supremum : sup(A) ile gösterilir.

Eğer A'nın bir alt sınırı, A'nın diğer bütün alt sınırlarını ilk izleyen ise buna A'nın infimumu denir.En Büyük Alt Sınır(Greatest Lower Bound = Infimum : inf(A)

En Büyük ortak Bölen (inf) , En küçük ortak kat(sup) bu tanımlara uyar.(Şekil 1.12.)



Şekil 1.12.

En büyük ve en küçük eleman

Teorem 1.18' e göre reel sayıların her hangi bir alt kümesi $\leq$ bağıntısı ile parçalı sıralıdır. Bu şekilde sıralanmış bazı reel sayı kümeleri en büyük veya en küçük elemana sahip olabilir, bazıları da olmayabilir. Örneğin, tam sayılar kümesinin en büyük veya en küçük elemanı yokken, pozitif tamsayıların en küçük elemanı 1' dir fakat en büyük elemanı yoktur.

En büyük veya en küçük eleman bir tane olmayabilir. Örneğin, {a,b,c} kümesinin öz alt kümelerini eleman sayısına göre sıralarsak, en küçük eleman $\varnothing$ iken en büyük eleman üç tanedir çünkü üç tane iki elemanlı alt küme vardır.

Tanım: ***R***, A kümesi üzerinde bir parçalı sıra olsun. A' nın **en büyük elemanı,** $\forall$ $a \in A$ için a ***R*** α olmak üzere α elemanıdır.

Benzer şekilde, A' nın **en küçük elemanı,** $\forall$ $a \in A$ için β ***R*** a olmak üzere β elemanıdır.

Yeniden {a,b,c}' nin öz alt kümeleri örneğine dönersek iki elemanlı her bir alt küme en büyük eleman olacaktır. O halde bu düşünceyi maksimal eleman tanımı ile formülize edebiliriz.

Tanım: A, ***R*** sıra bağıntılı bir parçalı sıralı küme olsun. $\forall$ $a \in A$ için x ***R*** a x=a anlamına geliyorsa A' daki x elemanı **maksimal**dir.

Benzer şekilde, $\forall$ $a \in A$ için a ***R*** y a=y anlamına geliyorsa y elemanı **minimal**dir.

1.5 Kafes Yapıları ve Özellikleri(Lattice Structures)

L üzerinde karşılaşma(meet) ve birleşme(join) adı altında iki ikili işlem tanımlanan boş olmayan küme;

Karşılaşma "$\wedge$" ; birleşme "$\vee$" birbirinin dualı. Ancak işlemler aşağıdaki aksiyomları sağlamalıdır.

L_1 : Değişme :$a \wedge b = b \wedge a$; $a \vee b = b \vee a$

L_2 : Birleşme :$(a \wedge b) \wedge c = a \wedge (b \wedge c)$; $(a \vee b) \vee c = a \vee (b \vee c)$

L_3: Yutma : $a \wedge (a \vee b) = a$; $a \vee (a \wedge b) = a$

Bu aksiyomlar birbirinin dualıdır. Buna göre diğer tanımlanacak özelliklerinde bir dualı vardır.

1: Sabit Kuvvetlilik(idempotence)

$a \wedge a = a$

$a \wedge a = a \wedge [a \vee (a \wedge b)]$

$= a \wedge (a \vee c) = a$

Teorem 1.19 : $a \wedge b = a \Leftrightarrow a \vee b = b$'dir.

$b = b \vee (b \wedge a)$ (yutma)

$b = b \vee a$

$a = a \wedge (a \vee b)$ (yutma)

$a = a \wedge b$ bulunur.

Teorem1.20 : L'de $a \wedge b = a$ $(a \vee b = b)$ şeklinde tanımlanan bağıntı bir sıra bağıntısıdır.

$a \wedge a = a$ Yansıma

$a \wedge b = a$ ve $b \wedge a = b \Rightarrow a = b$ (Antisimetri)

$a \wedge b = a$, $b \wedge c = b \Rightarrow a \wedge c = a$ geçiş,

Kafes bir kısmi sıralı kümedir denilebilir. Her POSET bir kafesmidir? Bu soruyu cevaplamak için aşağıdaki teoremin ispatı verilebilir.

Teorem 1.21. P (kısmi sıralı küme) her eleman çifti için (a,b) bir infimum ve bir supremum var olan bir kısmi sıralı küme ise, P bir kafes yapısıdır. Bu durumda;

$a \wedge b = Inf(a,b)$

$a \vee b = Sup(a,b)$ olarak tanımlanır

İspat: Inf. ve sup. ifadelerinin kafes aksiyomlarının sağlayıp sağlamadıklarına bakalım..

$inf(a,b) = inf(b,a)$; $\{ a \wedge b = b \wedge a \}$

$inf(inf(a,b),c) = inf(a, inf(b,c))$; $\{ (a \wedge b) \wedge c = a \wedge (b \wedge c) \}$

$inf(a,sup(a,b)) = a$ yazabiliriz. ; $\{ a \wedge (a \vee b) = a \}$

Bu aksiyomları sup. için de gerçekleyebiliriz. Böylece bu aksiyomlar tanımlandığına göre P kısmi sıralı kümesi bir kafestir

Alt Kafes: : $M \subseteq L$ (kafes) , M bir alt küme. M'nin alt kafes olabilmesi için M'nin $\wedge$, $\vee$ işlemlerine kapalı olması gerekir.

İzomorf Kafesler : (Aynı biçimde olan yapılar) L ve L' kafesler olmak üzere;

$\boldsymbol{f}$:L→ L' , $\boldsymbol{f}$ evrilebilir bir fonksiyon.

$\boldsymbol{f}(a \wedge b) = \boldsymbol{f}(a) \wedge \boldsymbol{f}(b)$ ise $\boldsymbol{f}$ fonksiyonu bir izomorfizmdir. Karşılaştırma işlemi de L ve L' nde bir izomorf kafes tanımlar. Düalite burada da geçerlidir.

Sınırlı Kafesler(Bounded Lattices) : Bir kafeste bir alt sınır varsa bunu o simgesi ile göstereceğiz. Bir üst sınır varsa bunu I ile göstereceğiz.

$\forall x \in L$, $o \leq x$;

$\forall x \in L$, $x \leq I$ şeklinde sınırları tanımlanabiliyorsa buna sınırlı kafes denir.

Kafeste eleman sayısı sonlu ise sınırlar vardır. Eğer o ve I mevcutsa, $\forall a \in L$ için;

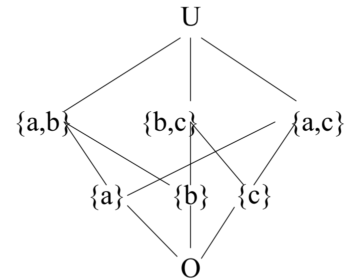
$a \vee I = I$; $a \vee o = a$

$a \wedge I = a$; $a \wedge o = o$

Teorem 1.22: Sonlu kafes sınırlıdır.

$a_1 \vee a_2 \vee a_3 \ldots\ldots\ldots\ldots \vee a_n = I$ dır.

$a_1 \wedge a_2 \wedge a_3 \ldots\ldots\ldots\ldots \wedge a_n = o$ dır.



Şekil 1.12

Örnek: U sonlu bir küme P(u) 'U'nun alt kümeler kümesi olsun.

$\subseteq$:Sıra bağıntısı(içine alma)

$\cap$:Kesişme karşılama

$\cup$: Birleşme bağıntıları olsun.

U= {a,b,c} dersek hasse diyagramı Şekil 1.12'deki gibi olur.

İşlemleri Dağılma Özelliği Gösteren Kafesler(Distribütif Lattice) :

$\forall a,b,c \in L$, için $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ ve;

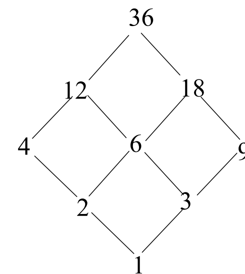
$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ yazılabiliyorsa böyle kafeslere distribütif kafesler denir.

Örnek 1.40: 36'nın bölenleri 12,6 ve 9'u alalım.

$12 \wedge (6 \vee 9) = (12 \wedge 6) \vee (12 \wedge 9)$

$12 \wedge 18 = 6 \vee 3$

6=6 Bütün elemanlar için bu yapılabilir.



Şekil 1.13

Karşı Örnek : Distribütif olmayan Kafes :Şekil 1.14 (a)

$a \vee (b \wedge c) = a$

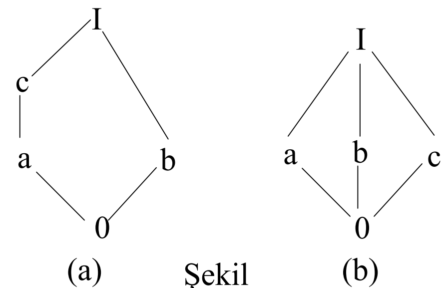
$(a \vee b) \wedge (a \vee c) =$

$I \wedge c = I$

Şekil 1.14 (b)

$a \vee (b \wedge c) = a$

$(a \vee b) \wedge (b \vee c) = I$



Şekil 1.14

Teorem 1.23: Şekil 1.14 de verilen örnek kafesten birini alt kafes olarak içine alan hiçbir kafes distribütif değildir.

Tanım: Elemanları tümlenen sonlu kafesler(alt sınır o, üst sınır I) x 'a'nın tümleyeni dir . O halde; $a \vee x = I$ ve $a \wedge x = o$ demektir.

Bir kafeste her elemanın tümleyeni olmayabilir. Bazı elemanların tümleyeni tek olmayabilir. Kafeste üst ve alt sınır muhakkak tektir.

Şekil 1.14(a) için : $c \vee b = I$; $c \wedge b = o$

$a \vee b = I$; $a \wedge b = o$ (c, a ve b' nin tümleyeni)

1.6 Fonksiyonlar ve Tanımları

x^2+5x-8, $1/(x+3)^3$, cos(x), log(x) vs. gibi ifadeler genellikle ***f***(x) ile gösterilir ve "x' in fonksiyonu" olarak adlandırılır. İfadenin kendisinden daha önemli olan verilen herhangi bir x değerine karşılık fonksiyonun değerini hesaplamak için bir kural tanımlamasıdır. İki farklı ifade ***f***(x) ve g(x), tüm x reel sayıları için aynı değerleri verebilir ve biz bu iki ifadenin aynı fonksiyonu tanımladığını söyleyebiliriz. Örneğin ***f***(x)=x^2+4x-5 ve ***g***(x)=$(x+2)^2-9$.

Tanım: A ve B iki küme olsun. A' dan B' ye bir ***f*** fonksiyonu; ***f***: A→B şeklinde yazılır ve her bir $a \in A$ 'yı tek bir ***f***(a)$\in$B elemanı ile eşleştiren bir kuraldır.

Örnek 1.41: x^2+4x-5 ifadesi tek başına bir fonksiyon değildir zira tanımıza göre A ve B kümeleri belirtilmemiştir. Öte yandan, bu ifade şu şekilde tanımlanabilir: ***f***: R → R olmak üzere ***f***(x)=x^2+4x-5.

Tanım: A ve B küme olsun. ***f***, A' dan B' ye bir fonksiyon ***f***: A→B şeklinde yazılır ve ***f***$\subseteq$(AxB) 'nin alt kümesidir ve şu kuralı sağlar:

Her bir $a \in A$ için $(a,b) \in$ ***f*** olmak üzere tek bir $b \in B$ vardır. ($\forall a \in A$ 'yı ***f*** (a)$\in$B 'de tek bir elemana eşleştiren bir kuraldır)

A kümesi ***f***' nin tanım kümesi ve B kümesi de ***f***' nin değer kümesi denir. $(a,b) \in$ ***f*** ise $b \in B$ elemanı $a \in A$ elemanının görüntüsüdür denir ve b=***f***(a) veya ***f***: $a \mapsto b$ şeklinde yazılır.

Tanım: ***f***: A→B ve g: A'→B' fonksiyonları

(i) A=A'

(ii) B=B'

(iii) ***f***(a)=***g***(a) (A=A' 'ne ait tüm a elemanları için)

ise eşittir.

Bir fonksiyonun grafiği R^2= R x R düzleminde y=***f***(x)' i sağlayan (x,y) noktalarını içeren eğridir. Ancak unutulmaması gereken nokta x-y düzlemindeki her eğri her hangi bir ***f***: A→IR (A$\subseteq$ R) fonksiyonun grafiği değildir. Örneğin, merkezi orijin (0,0), yarıçapı 1 olan çemberin denklemi $x^2+y^2=1$' dir. -1 ve 1 arasındaki her bir x değeri için iki tane y değeri vardır.

(x,y)-düzleminde verilen bir eğrinin bir fonksiyonun grafiği olup olmadığını anlamak

kolaydır. x=a dikey doğrusu sadece ve sadece eğriyi tek bir yerde kesiyorsa, verilen $a \in A$ için $y=f(a)$ olacak şekilde tek bir $y \in$ R vardır.

Bir fonksiyonun tanımında karışıklığa sebep olan iki özellik vardır. Birincisi, tanım kümesinin iki veya daha fazla elemanı değer kümesinde aynı görüntüye sahipse. İkincisi ise, değer kümesindeki tüm elemanların, tanım kümesindeki bir elemanın görüntüsü olmak zorunda olmadığıdır.

Tanım: ***f***: A→B bir fonksiyon olsun. ***f*' nin görüntüsü** (aralığı)

$$\mathrm{im}(f)=\{b \in B: (a,b) \in f,\ a \in A \text{ için}\}$$ kümesidir.

Dikkat edilirse im(***f***) değer kümesi B' nin alt kümesidir ve $a \in A$ elemanının görüntüsü ***f***(a) ile karıştırılmamalıdır. Bir elemanın görüntüsü bir elemandır fakat bir fonksiyonun görüntüsü bir kümedir ; bir başka deyişle tanım kümesindeki elemanların görüntülerinin tamamını içeren kümedir.

$$\mathrm{im}(f)=\{f(a): a \in A\}.$$

Örnek 1.42: ***f***: R→R olmak üzere $f(x)=\dfrac{3x}{x^2+1}$ fonksiyonunun görüntüsünü bulunuz.

Çözüm: Tanıma göre $y \in \mathrm{im}(f)$ sadece ve sadece $x \in$ R için $y=\dfrac{3x}{x^2+1}$ ise.

Bu eşitlik şuna eşittir: $yx^2+y=3x$ veya

$$yx^2-3x+y=0.$$

Bu durumda $x=\dfrac{3 \pm \sqrt{9-4y^2}}{2y}$ olur.

Bu nedenle gerçek çözüm $y \neq 0$ ve $9-4y^2 \geq 0$ olmalıdır.

Böylece $y^2 \leq 9/4$ yani $-3/2 \leq y \leq 3/2$ (ve $y \neq 0$) elde edilir.

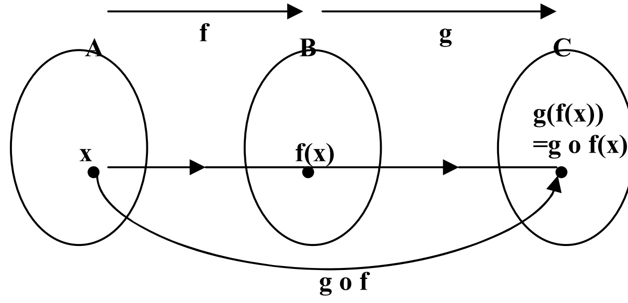
Bu durumda $-3/2 \leq y \leq 3/2$, $y \neq 0$ sağlandığında $y=f(x)$ olacak şekilde bir x reel sayısı bulunabilir. y=0 özel bir durumdur fakat açıkça $f(0)=0$' dır o halde, $0 \in \mathrm{im}(f)$ ' dir.

Böylece, $\mathrm{im}(f)=[-3/2, 3/2]=\{y \in \mathrm{R}: -3/2 \leq y \leq 3/2\}$.

f:A→R gibi bir fonksiyonun grafiği verilmişse bu fonksiyonun görüntüsü kolayca bulunabilir. A' nın her bir elemanının görüntüsü ***f***(a); a' dan grafiği kesene kadar dikey doğru çizerek ve sonra kesişim noktasından da y-eksenine yatay bir doğru çizerek bulunabilir.

1.6.1 Bileşik Fonksiyonlar, Birebir(injective) ve Örten(Surjektive) fonksiyonlar

f: A→B ve ***g***: B→C iki fonksiyon olsun. x, A'nın elemanı ise y=***f***(x) B' ye aittir. Bu nedenle ***g***(y)=***g***(***f***(x)) C' nin elemanıdır. A 'dan C' ye bir fonksiyon tanımlamak için ***f*** ve ***g*** 'nin bileşkesi dediğimiz ve $g \circ f$ ile gösterdiğimiz $x \mapsto g(f(x))$ ortaklığını kullanabiliriz. $g \circ f$ bileşik fonksiyonu Şekil 1.15'deki gibi gösterilebilir.



Şekil 1.15. Bileşik fonksiyon

Tanıma göre $g \circ f$ fonksiyonu z= $g \circ f$(x) olacak şekilde tüm (x,z) elemanlarını içeren A x C kartezyen çarpımının alt kümesi olmalıdır. y=f(x)$\in$B dersek (x,y) $\in f$ ve (y,z) $\in g$ 'dir. Bu nedenle, bileşik fonksiyonları şu şekilde tanımlarız.

Tanım: f: A→B ve g: B→C iki fonksiyon olsun. **Bileşik fonksiyon** $g \circ f$: A→C:

$g \circ f$={(x,z) $\in$ A x C: (x,y)$\in f$ ve (y,z)$\in g$ (y$\in$Biçin)}

İki rastgele fonksiyonun bileşkesi $g \circ f$ olmayabilir. Yukarıdaki tanıma göre g' nin tanım kümesi, f' in değer kümesine eşittir. Ancak bu kati bir kural değildir. $g \circ f$ tanımını biraz genişletirsek:

f: A→B ve g: B'→C iki fonksiyon ve a$\in$A olsun. $g(f$(a))' nın tanımlı olabilmesi için f(a)'nın g' nin tanım kümesi olan B' kümesine ait olması gerekir. Bu durumda $g \circ f$ 'i tanımlamak için $g(f$(a))' nın tüm a$\in$A için tanımlı olması şarttır. Böylece $g \circ f$ sadece ve sadece f' in görüntüsü g' nin tanım kümesinin alt kümesi ise tanımlıdır. Tabii ki, bu şart yukarıdaki tanımda olduğu gibi B=B' ise sağlanır.

Örnek 1.43: f ve g R→R ve f(x)=x+2, g=1/(x^2+1) şeklinde tanımlı olsun. Bu durumda,

$$g \circ f(x) = g(f(x))$$
$$= g(x+2)$$
$$= \frac{1}{(x+2)^2+1}$$
$$= \frac{1}{x^2+4x+5}$$

Benzer şekilde;

$$f \circ g(x) = f(g(x))$$
$$= f(1/(x^2+1))$$
$$= \frac{1}{x^2+1}+2$$
$$= \frac{2x^2+3}{x^2+1}$$

Bu örnek gösteriyor ki, genellikle $f \circ g \neq g \circ f$.

Teorem 1.26: f: A→B ve g: B→C iki fonksiyon olsun. Bu durumda im($g \circ f$)$\subseteq$im(g).

İspat: c$\in$im($g \circ f$) olsun. O halde, ($g \circ f$)(a)=$g(f$(a))=c olacak şekilde a$\in$A mevcuttur. Bu

durumda, b=$\boldsymbol{f}$(a)$\in$B dersek $\boldsymbol{g}$(b)=c' dir ve bu nedenle c$\in$im($\boldsymbol{g}$)' dir. Bu sebeple, im($\boldsymbol{g}\circ\boldsymbol{f}$)$\subseteq$im($\boldsymbol{g}$).

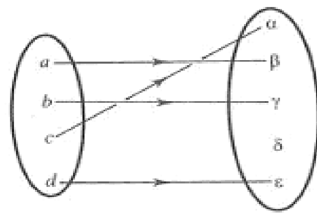
Önceki bölümlerden hatırlayacağımız gibi bir $\boldsymbol{f}$: A→B fonksiyonu

(i) tanım kümesinin farklı elemanları aynı görüntüye sahip olabilir.

(ii) değer kümesinin bazı elemanları tanım kümesinin herhangi bir elemanının görüntüsü olmayabilir.

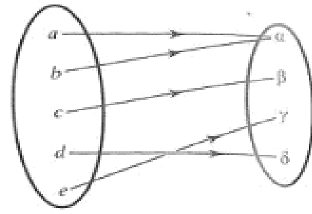
Örneğin, $\boldsymbol{f}$: R→R, $\boldsymbol{f}$(x)=x^2 fonksiyonunda bu iki olasılık da mümkündür. Hem 2 hem de -2 aynı görüntüye sahip olduğu gibi herhangi bir negatif reel sayı $\boldsymbol{f}$' in görüntüsüne dahil değildir.(tüm x reel sayıları için $x^2 \geq 0$).

Yukarıdaki maddelerden ilkinin mümkün olmadığı fonksiyonlara birebir (injective), ikincisinin mümkün olmadığı fonksiyonlara da örten (surjective) denir. Bu iki durum 1.16' da gösterilmiştir. Şekil 1.14 (a) 'daki $\boldsymbol{f}$:{a,b,c,d}→{$\alpha,\beta,\gamma,\delta,\varepsilon$} fonksiyonu injective'dir fakat surjective değildir. Diğer yandan, şekil 1.14 (b) 'deki g:{a,b,c,d,e}→{$\alpha,\beta,\gamma,\delta$} fonksiyonu surjective'dir fakat injective değildir.



(a) injektif

Tanım kümesinin farklı elemanları farklı görüntüye sahip



(b) sürjektif

Değer kümesinin tüm elemanları tanım kümesinin bir elemanının görüntüsü

Şekil 1.16.

Tanım: $\boldsymbol{f}$: A→B bir fonksiyon olsun.

(i) Tüm a, a'$\in$A elemanları için aşağıdaki durum sağlanıyorsa $\boldsymbol{f}$ birebir(injective)dir veya bir injeksiyon(birebir fonksiyon)dur deriz:

Eğer (a,b), (a',b')$\in\boldsymbol{f}$ ve a$\neq$a' ise b$\neq$b'.

(ii) Eğer her b$\in$B için (a,b)$\in\boldsymbol{f}$ olacak şekilde a$\in$A mevcut ise $\boldsymbol{f}$ örten(surjective)dir veya bir örten fonksiyon(surjeksiyon)dur deriz.

Örnek 1.44: $\boldsymbol{f}$: R→R, $\boldsymbol{f}$(x)=3x-7 olsun. f' in hem birebir hem de örten fonksiyon olduğunu gösteriniz.

Çözüm: $\boldsymbol{f}$' in birebir olduğunu göstermek için tüm x ve y reel sayıları için $\boldsymbol{f}$(x)=$\boldsymbol{f}$(y) 'nin x=y anlamına geldiğini ispatlamamız gerekir.

$\boldsymbol{f}$(x) = $\boldsymbol{f}$(y)

3x-7 = 3y-7

3x = 3y

x = y. O halde f birebir dir.

$\boldsymbol{f}$' in örten olduğunu göstermek için, y 'nin R değer kümesinin herhangi bir elemanı olduğunu

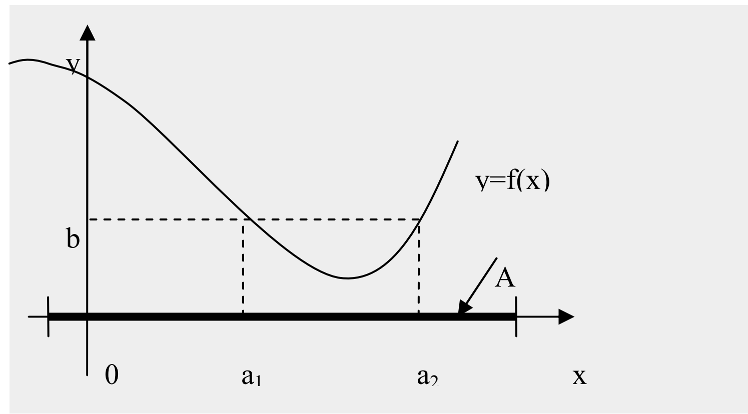
düşünelim. $f(x)=y$ olacak şekilde $x\in R$ bulmamız gerekir. $x=(y+7)/3$ olsun. O halde, $x\in R$ ve

$$f(x) = f((y+7)/3)$$
$$= 3.\frac{y+7}{3}-7$$
$$= y+7-7$$
$= y$. O halde f örtendir.

Bu ispat herhangi bir **doğrusal fonksiyon**un f: R→R, $f(x)=ax+b$ hem birebir hem de örten olduğunu göstermek için kullanılabilir.

A ve B, R' nin alt kümeleri olmak üzere f: A→B fonksiyonu olsun. Bir fonksiyonun grafiğinden birebir veya örten olup olmadığını anlayabiliriz.

f ' in birebir olmadığını farz edelim. O halde, A' da $f(a_1)=f(a_2)=b$ olacak şekilde iki tane a_1 ve a_2 elemanı vardır. Bunun anlamı b 'den çizilen yatay doğru x-eksenini $x=a_1$ ve $x=a_2$ 'de keser. Bu durum şekil 1.17'de gösterilmiştir.



Şekil 1.17.

Öte yandan eğer f birebir ise bu durum hiçbir zaman gerçekleşmez. Yani yatay doğru grafiği birden fazla yerden kesmez.

Örten özelliği ise şu şekildedir: im(f)=B olmak üzere f, sadece ve sadece B' nin bir noktasından geçen her yatay doğru grafiği en az bir kere kesiyorsa örtendir.

Teorem 1.27: f: A→B ve g: B→C iki fonksiyon olsun.

(i) Eğer f ve g her ikisi birden birebir ise $g\circ f$ de birebir'dir.

(ii) Eğer f ve g her ikisi birden örten ise $g\circ f$ de örten'dir.

İspat: (i) f ve g' nin birebir fonk. olduğunu düşünelim. a, a'$\in$A, b=f(a) ve b'=f(a') olsun. Bu durumda,

$g\circ f(a)=g\circ f(a')$

$\Rightarrow$ $g(f(a)) = g(f(a'))$

$\Rightarrow$ $g(b) = g(b')$

$\Rightarrow$ b = b' (zira g birebirdir.)

$\Rightarrow$ $f(a) = f(a')$ (çünkü $f(a)=b$, $f(a')=b'$.)

$\Rightarrow$ a = a' (zira f birebirdir.)

Böylece $g \circ f$ bir birebir fonk.dur.

Teorem 1.28: f: A→B ve g: B→C iki fonksiyon olsun.

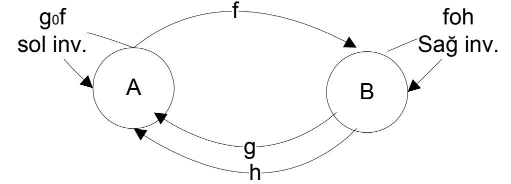
(i) $g \circ f$ bileşik fonksiyonu birebir ise f de birebirdir.

(ii) $g \circ f$ bileşik fonksiyonu örten ise g de örtendir.

Tanım(Özdeşlik Fonksiyonu): id_A: A→A fonksiyon, id_A:{(x,x):x∈A}, $id_A(x)=x$ x∈A dır.

Teorem 1.29: (i) f: A→B fonksiyonu sadece ve sadece $g \circ f = id_A$: A→A (A'nın özdeşlik fonksiyonu) olacak şekilde bir g: B→A varsa birebir'dir.

(ii) f: A→B fonksiyonu sadece ve sadece $f \circ h = id_B$: B→B (B'nın özdeşlik fonksiyonu) olacak şekilde bir h: B→A varsa birebir'dir.



Şekil 1.18.

Tanım: f: A→B herhangi bir fonksiyon olsun. $g \circ f = id_A$ olacak şekilde bir g: B→A fonksiyonu f için bir **sol inverse**, benzer şekilde $f \circ h = id_B$ olacak şekilde bir h: B→A fonksiyonu f için bir **sağ inverse** denir.

1.6.2 Ters Fonksiyonlar

Hem birebir hem de örten fonksiyonlar ilginç ve önemli özelliklere sahiptir.

Tanım: f: A→B fonksiyonu hem birebir hem de örten ise birebir ve örten(bijective)dir veya bijeksiyondur.

Teorem 1.30: A ve B IR' nin alt kümeleri olmak üzere f: A→B fonksiyon olsun. O halde f, sadece ve sadece B' nin bir noktasından çizilen her doğru f' nin grafiğini tam olarak bir yerde kesiyorsa birebir ve örten'dir.

Teorem 1.31: (i) İki birebir ve örten fonksiyonun bileşkesi yine birebir ve örten fonk.dur.

(ii) f: A→B fonksiyonu sadece ve sadece hem sol hem de sağ inverse' e sahipse birebir ve örten fonk.dur.

(iii) A ve B sonlu kümeler olmak üzere f: A→B bijeksiyon ise $|A| = |B|$.

Dikkat edilirse (i) şıkkının tersi yanlıştır. Eğer bir bileşik fonksiyon $g \circ f$ birebir ve örten ise hem f hem de g birebir ve örten olmak zorunda değildir. Eğer A ve B aynı kardinaliteye sahip sonlu kümeler ise A' dan B' ye bir birebir ve örten fonk. vardır.

Şimdi şu soruya bir göz atalım. f: A→B şeklinde verilmiş bir fonksiyon olsun. g={(b,a):(a,b)∈f} hangi durumlarda bir fonksiyon tanımlar? Burada g' yi f' in diyagramında okları tersine çevirmek gibi düşünebiliriz: Eğer b=f(a) ise a=g(b) 'dir.

Genel duruma bakacak olursak, f: A→B bir fonksiyon ve g={(b,a):(a,b)∈f} şeklinde tanımlanmış olsun. O halde g, her bir b∈B için (b,a)∈g veya (a,b)∈f olacak şekilde tek bir a∈A varsa fonksiyondur. B' nin her bir elemanı için gerekli özellikleri sağlayan a' ların varlığı aynı zamanda f' in örten olması için aranan şartlardır. Bunun da ötesinde, (a,b)∈f olacak şekilde bir a∈A elemanı sadece ve sadece f birebir ise tektir.

Teorem 1.32: f:A→B bir fonksiyon olsun. g={(b,a)∈B x A: (a,b)∈f} bağıntısı sadece ve sadece f birebir ve örten ise B' den A' ya bir fonksiyondur.

Tanım: f:A→B bir birebir ve örten fonk. ise g: B→A, 'g(b)=a sadece ve sadece f(a)=b ise'

şeklinde tanımlanan fonksiyona ***f*'** in ters fonksiyonu denir ve f^{-1} şeklinde gösterilir.

Teorem 1.33: f:A→B bir bijeksiyon ise f^{-1}:B→A f için hem sol hem de sağ inverse' tür.

Örnek 1.45: ***f***: R -{1}→ R -{2}, ***f***(x)=$\frac{2x}{x-1}$ fonksiyonunun birebir ve örten olduğunu gösterin ve tersini bulun.

Çözüm: Eğer f^{-1} 'i bulabilirsek ***f*** birebir ve örten olmalıdır. f^{-1}' i bulabilmek için tanımı kullanırız: y=***f***(x) ise x=f^{-1}(y). O halde,

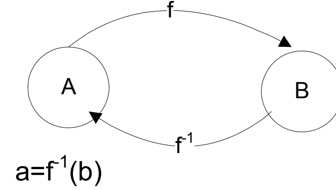
y=$\frac{2x}{x-1}$

⇒ y(x-1)=2x

⇒ yx-2x=y

⇒ x(y-2)=y

⇒ x=$\frac{y}{y-2}$



Şekil 1.19.

Bu sebeple şu fonksiyonu tanımlayabiliriz:

g: R -{2}→ R -{1}, ***g***(y)=y/y-2.

1.7 Boole cebri ve mantıksal Fonksiyonlar

1.7.1 Bole cebrinin özellikleri

Sayısal bilgisayarlar ve sayısal elektronik devreler ikili sayı sistemini kullanarak işlem yaparlar. İkili sistemde kullanılan sayılar ise 1 ve 0'dan ibarettir. Boole cebri {0,1} kümesini kullanarak işlemler ve kurallar tanımlar. Boole cebrinde , en çok kullanılan üç işlem eşlenik, mantıksal toplama ve mantıksal çarpma 'dır. Eşlenik işleminde $\overline{1}$=0; $\overline{0}$ =1 olur.

Bir boole cebri sınırlı, dağılma özellikli, her öğenin bir tümleyeni olan bir kafes yapıdır.

∨ için + lojik (mantıksal toplama, OR) kullanılır. aşağıdaki değerleri alır

1+1 = 1 ; 1+0 = 1; 0+1= 1; 0+0 = 0

; ∧ için • lojik (mantıksal çarpma, AND) kullanılır. aşağıdaki değerleri alır

1•1 = 1 ; 1•0 = 0; 0•1= 0; 0•0 = 0

1.7.2 Boole Cebrinin Fonksiyonları

.B = {0,1} verilsin. Eğer x değişkeni sadece B'den değerler alırsa x'e mantıksal değişken adı verilir. $\{x_1,x_2,.........,x_n \mid x_i \in B, 1 \leq i \leq n\}$ olmak üzere, B^n'den B'ye tanımlanan bir fonksiyona n. Dereceden mantıksal fonksiyon denir. Mantıksal fonksiyonun alacağı değerler çoğunlukla tablolar şeklinde gösterilir. Örneğin, x=1 ve y=0 iken *F*(x,y) nin değeri 1'dir. Diğer değerler Tablo 1.5'de gösterilmiştir.

x	y	***F***(x,y)
1	1	0
1	0	1
0	1	1
0	0	0

Tablo 1.5.

Mantıksal fonksiyonlar, değişkenler ve mantıksal işlemlerden oluşan ifadeler kullanılarak gösterilebilir. Mantıksal ifadeler, $x_1,x_2,.........,x_n$ değişkenleriyle rekürsif olarak aşağıdaki şekilde ifade edilebilir

$0,1,x_1,x_2,.........,x_n$, 'ler mantıksal ifadelerdir;

eğer E_1 ve E_2 mantıksal ifadeler ise , $\overline{E_1}$, (E_1E_2) ve (E_1+E_2) de mantıksal ifadelerdir.

n değişkenli ***F*** ve ***G*** mantıksal ifadeleri ancak ve ancak $\boldsymbol{F}(b_1,b_2,..........,b_n) = \boldsymbol{G}(b_1,b_2,..........,b_n)$ ise eşdeğerdir. ($b_1,b_2,..........,b_n \in$ B) Aynı fonksiyonu temsil eden iki farklı mantıksal ifade eşdeğer olarak adlandırılır. Örneğin xy, xy+0 ve xy.1 eşdeğerdir. F mantıksal fonksiyonunun eşleniği $\overline{F}$ fonksiyonudur. Burada, $\overline{F}(x_1,x_2,.........,x_n) = \overline{F(x_1,,,,,,,,,,x_n)}$ dir. ***F*** ve ***G***, n. Dereceden mantıksal fonksiyonlar olsun. Mantıksal toplam (***F***+***G***) ve mantıksal çarpım(***F***.***G***) aşağıdaki şekilde tanımlanır.

$(\boldsymbol{F}+\boldsymbol{G})(x_1,x_2,.........,x_n)= \boldsymbol{F}.(x_1,x_2,.........,x_n) + \boldsymbol{G}(x_1,x_2,.........,x_n)$,

$(\boldsymbol{F}.\boldsymbol{G})(x_1,x_2,.........,x_n) = \boldsymbol{F}. F(x_1,x_2,.........,x_n)\ \boldsymbol{G}(x_1,x_2,.........,x_n)$

derecesi iki olan mantıksal fonksiyon , B = {0,1} den eleman çiftlerinin oluşturduğu 4 elemanlı kümeden B 'ye bir fonksiyondur. Buradan 2.dereceden 16 adet mantıksal fonksiyon tanımlanabilir. Tablo 1.6'de F_1,F_2, ...F_{16} nın değerleri görülmektedir.

x	x	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9	F_{10}	F_{11}	F_{12}	F_{13}	F_{14}	F_{15}	F_{16}
1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
1	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0
0	1	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0

Tablo 1.6.

Tanım: Derecesi n olan mantıksal fonksiyon sayısı 2^{2^n} adettir. 1 : 4 ; 2 : 16 ; 3 : 256 ...)

Boole Cebrinin Özellikleri

Boole cebrinin birçok özelliği vardır. Bunların önemlileri tablo 1.7'de gösterilmiştir.

Özellik	Açıklama
$\overline{\overline{x}} = x$	Çift eşlenik kuralı
$x+x = x$ $x.x=x$	Sabit kuvvetlilik(Idempotence) kuralı
$x+0 = x$ $x.1=x$	Eşlik elemanı kuralı
$x+1 = 1$ $x.0=0$	Baskınlık kuralı
$x+y = y+x$ $x.y=y.x$	Değişme kuralı
$x+(y + z)= (x+y)+z$ $x.(y.z)=(xy)z$	Birleşme kuralı
$x+yz= (x+y)(x+z)$ $x(y+z)= xy+xz$	Dağılma kuralı
$\overline{(xy)} = \overline{x} + \overline{y}$; $\overline{(x+y)} = \overline{x}\,\overline{y}$	De Morgan Kuralı
$x+\overline{x} = 1$; $x.\overline{x} = 0$	Tümleyen eleman(complement)

Tablo 1.7.

Kuralların ispatı doğruluk tabloları yapılarak gerçeklenebilir. Ayrıca bu kurallar VEYA (OR +) ve VE(AND .) işlemleriyle de yazılabilir.

Düalite kuralı : Bir boole ifadesinin dualı mantıksal çarpım ile toplamların ve 1 ile 0 'ların yer değiştirmesiyle elde edilir.

Örnek1.32: x(y+0) 'ın düali x+(y.1) ve $\bar{x}.1+(\bar{y}.z)$ in düali $(\bar{x}+0)(\bar{y}z)$ dir.

1.7.3 Mantıksal Fonksiyonların Gösterilmesi

Değişkenlerinin almış oldukları değerlere karşılık olarak elde edilecek olan mantıksal fonksiyonun gösterilmesi önemlidir. Bir mantıksal fonksiyon üç mantıksal operatör olan + . ve ¯ ile gösterilebilir. Bu bölümde önce mantıksal fonksiyonların gösterilmesi daha sonra da mantıksal fonksiyonların en küçük değişken kümesi ile gösterilmesi(indirgenmesi) açıklanacaktır. Bu gösterilimler mantıksal devre tasarımında önemlidir.

Tablo 1.8.

x	y	z	***F***	***G***
1	1	1	0	0
1	1	0	0	1
1	0	1	1	0
1	0	0	0	0
0	1	1	0	0
0	1	0	0	1
0	0	1	0	0
0	0	0	0	0

Çarpımlar toplamı

Tablo 1.8.'de gösterilen *F*(x,y,z) ve ***G***(x,y,z) fonksiyonlarının bulunması

F fonksiyonunun değeri x=z=1 ve y = 0 iken 1 değerini almaktadır. Diğer giriş değerlerinde 0 olmaktadır.Böyle bir ifade x, $\bar{y}$ ve z mantıksal çarpımı olan x.$\bar{y}$.z ile temsil edilebilir.

G'nin bulunması ise, x=y= $\bar{z}$ =1 veya $\bar{x}$ =y= $\bar{z}$ =1 durumunda 1 değerini alır diğerlerinde 0 olur. Bu durumda çarpımlar toplamı olarak

G(x,y,z)=x.y.$\bar{z}+\bar{x}$.y.$\bar{z}$ elde edilir.

Tanım: (Minterm) : Mantıksal $x_1,x_2,.........,x_n$ değişkenlerinin bir mintermi $y_1y_2........y_n$ çarpımıdır. Burada $y_i = x_i$ veya $y_i= \bar{x}_i$ dir. Bir minterm değişkenlerin almış oldukları değer sonucunda 1 değerini alır. Diğer bir deyişle $y_1y_2........y_n$ mintermi ancak ve ancak her bir y_i' nin değeri 1 ise 1 sonucunu verir. Bir mantıksal fonksiyon ise mintermlerin toplamı şeklinde ifade edilebilir.

Örnek 1.46: ***F***(x,y,,z) = (x+y) $\bar{z}$ fonksiyonunu çarpımlar toplamı şeklinde ifade ediniz.

Çözüm. İlk adım ***F*** fonksiyonunun değerinin bulunmasıdır. Bunun için Tablo 1.9 oluşturulur.

x	y	z	x+y	$\bar{z}$	(x+y) $\bar{z}$
1	1	1	1	0	0
1	1	0	1	1	1
1	0	1	1	0	0
1	0	0	1	1	1
0	1	1	1	0	0
0	1	0	1	1	1
0	0	1	0	0	0
0	0	0	0	1	0

Tablo 1.9.

F fonksiyonunun mantıksal eşdeğeri, fonksiyonun değerinin 1 olduğu durumlardaki değişkenlerin çarpımları 1 olacak şekilde çarpımlar toplamı şeklinde aşağıdaki ifade edilir.

F(x,y,,z) = $x.y.\bar{z}+x.\bar{y}.\bar{z}+\bar{x}.y.\bar{z}$

Tanım : maxterm : Mantıksal $x_1,x_2,.........,x_n$ değişkenlerinin bir maxtermi $y_1+y_2+........+.y_n$ toplamıdır. Burada $y_i = x_i$ veya $y_i= \bar{x}_i$ dir. Bir maxterm değişkenlerin almış oldukları değer sonucunda 0 değerini alır. Diğer bir deyişle $y_1+y_2+........+.y_n$ maxtermi ancak ve ancak her

bir y_i' nin değeri 0 ise 0 sonucunu verir. Bir mantıksal fonksiyon ise maxtermlerin çarpımı şeklinde ifade edilebilir.

1.7.4 Boole İfadelerinin Minimize Edilmesi

Mantıksal fonksiyonlar ile tasarlanan mantık devrelerinde kullanılan elemanların sayısının en küçüklenmesi ve aynı zamanda eşdeğer mantıksal fonksiyonu sağlaması tasarımda önemli bir mühendislik problemidir. Bu nedenle mantıksal fonksiyonların eşdeğeri olan ve en az mantıksal devre elemanı ile gerçeklenebilen fonksiyonun bulunması gereklidir. Çarpımlar toplamı olarak ifade edilen aşağıdaki fonksiyonun eşdeğerini hesaplayalım.

$\boldsymbol{F}(x,y,,z) = x.y.z+x.\bar{y}.z$

$= (y.+\bar{y})(xz)$

$=1.(xz) = xz$

Buradan ilk mantıksal ifade iki çarpma ve bir toplama elemanı ile gerçeklenebilirken indirgenen ifade tek çarpma elemanı ile gerçeklenebilmektedir.

İfadelerin indirgenmesi için iki adet yöntem kullanılır. Bunlar Karnaugh haritaları ve Quine-McCluskey Yöntemidir. Bu bölümde önce mantıksal ifadelerin indirgenme yöntemlerinin esasları anlatılacaktır.

Karnaugh Haritası Yöntemi

Bu yöntemde mintermlere eşdeğer olan en kısa ifade hesaplanır. Yöntem iki, üç, dört, vs. değişkenli ifadeler için farklı harita oluşturulmasını gerektirir. Tablo 1.10(a)'da iki değişkenli mantıksal ifadenin karnaugh haritası görülmektedir.

Örnek 1.47: $\boldsymbol{F}(x,y) = x.\bar{y} + \bar{x}.y$ nin haritası tablo 1.10(b) de , $x.\bar{y} + \bar{x}.y + \bar{x}\,\bar{y}$ nin ki ise 1.10(c) 'de görülmektedir.(b) nin eşdeğeri yine kendisi (c)'nin ki ise $\bar{x} + \bar{y}$ olarak elde edilir

	y	$\bar{y}$
x	xy	x$\bar{y}$
$\bar{x}$	y$\bar{x}$	$\bar{x}\,\bar{y}$

Tablo 1.10(a)

	y	$\bar{y}$
x		1
$\bar{x}$	1	

(b)

	y	$\bar{y}$
x		1
$\bar{x}$	1	1

(c)

Tablo 1.11(a)'da üç değişkenli mantıksal ifadenin karnaugh haritası görülmektedir.

Örnek 1.48:$\boldsymbol{F}(x,y,z) = \bar{x}y.z + x.\bar{y}z + x\bar{y}\bar{z} + \bar{x}\bar{y}z + \bar{x}\bar{y}\bar{z}$ 'nin haritası tablo 1.11(b) de , $xyz + xy\bar{z} + \bar{x}y.z + x.\bar{y}z + x\bar{y}\bar{z} + \bar{x}\bar{y}z + \bar{x}\bar{y}\bar{z}$ nin ki ise 1.11(c) 'de görülmektedir.(b) nin eşdeğeri $\bar{y} + \bar{x}z$, (c)'nin ki ise $x + \bar{y} + z$ olarak elde edilir.

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
x	xyz	$xy\bar{z}$	$x\bar{y}\bar{z}$	$x\bar{y}z$
$\bar{x}$	$\bar{x}yz$	$\bar{x}y\bar{z}$	$\bar{x}\bar{y}\bar{z}$	$\bar{x}\bar{y}z$

Tablo 1.11(a)

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
x			1	1
$\bar{x}$	1		1	1

(b)

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
x	1	1	1	1
$\bar{x}$	1		1	1

(c)

4 ve daha fazla değişkenli mantıksal ifadelerin indirgenmesi benzer şekilde karnaugh haritasının genişletilmesiyle yapılabilir. Ana kural, mintermlerde toplama giren eşlenik terimlerin haritada

daire içerisine alınması ve grupta değişmeyen terimin sonuçta yer almasıdır.

Karnaugh haritası pratik bir yöntem olmasına karşılık dörtten fazla değişkenli ifadelerde haritanın boyutu çok büyüyeceğinden tablo oluşturmak zorlaşır. Bu nedenle Quine-McCluskey yöntemi böyle ifadelerin indirgenmesinde kullanılabilir.Yöntemde mintermler en fazla 1 içeren bir dizilerine göre sırlanarak bu terimlerden indirgenme yapılır.

Örnek 1.49: $\boldsymbol{F}(x,y,z) = x.y.z + x\,\bar{y}\,z + \bar{x}\,y.z + \bar{x}\,\bar{y}\,z + \bar{x}\,\bar{y}\,\bar{z}$ ifadesinin indirgenmesini ele alalım. Bunun için Tablo 6.8 teşkil edilir. Tablo 1.12.'de adım 1 ve 2'den indirgenen terimlerin toplamı fonksiyonun indirgenmiş değeridir. 1. Adımda birbiriyle indirgenen terim numaraları gösterilmiştir. 2. adımda ise 1. adımdaki sonuçlardan birbiriyle indirgenen terimler gösterilmiştir. İndirgenemeyen terimler 1. adımda 5. terim 2. adımda ise ilk terimdir. Yani ifadenin indirgenmiş şekli $\boldsymbol{F}(x,y,z) = z + \bar{x}\,\bar{y}$ dir.

			1. Adım			2. Adım		
	Terim	Bit dizisi		Terim	Dizi		Terim	Dizi
1	$x.y.z$	111	(1,2)	$x.z$	1-1	(1,2,3,4)	z	--1
2	$x.\bar{y}\,z$	101	(1,3)	$y\,z$	-11			
3	$\bar{x}\,y.z$	011	(2,4)	$\bar{y}\,z$	-01			
4	$\bar{x}\,\bar{y}\,z$	001	(3,4)	$\bar{x}\,z$	0-1			
5	$\bar{x}\,\bar{y}\,\bar{z}$	000	(4,5)	$\bar{x}\,\bar{y}$	00-			

Tablo 1.12

1.8 Sayı ve Kodlama Teorisi ve Uygulamaları

1.8.1 Sayı Teorisine Giriş

Bu bölümde kriptolama algoritmalarının matematik modellemesinde kullanılan modüler aritmetik kavramları üzerinde kısaca durulacaktır.

Grup Teorisi

Tanım(Grup): Her bir elemanın tersinin olduğu monoide (G, *) **grup** denir. Yani (G, *) çifti şu dört şartı sağlar:

(G_1) *, Kapalılık, Eğer a ve b $\in$ G ise a*b $\in$ G dir.

(G_2) *, G üzerinde birleşme özelliğine sahiptir. $\forall$a,b,c $\in$ G için, a*(b*c) = (a*b)*c dir.

(G_3) bir etkisiz eleman mevcuttur. $\forall$a $\in$ G için, a*e = e*a =a dır.

(G_4) G' nin her bir elemanının tersi mevcuttur.$\forall$a$\in$G için,G'de bir a' vardır ve a*a'= a'*a =e dır.

Bu bölümde ve bundan sonraki bölümlerde belirtilmemiş ikili işlemler içeren ifadeler yazarken * simgesini göz ardı edeceğiz. Sadece yanlış anlamalara imkân verecek iki ikili işlemi birbirinden ayırt etmek için kullanacağız. Örneğin x*y yerine xy yazacağız (ancak çarpma işlemi ile

karıştırmamalıyız). Ayrıca aşağıdaki gibi x' in üslerini tanımlayacağız.

$n \in Z^+$ olmak üzere $x^n=x*x*\ldots*x$ (n tane)

ve $x \in Z^-$ olmak üzere $x^n=(x^{-1})^{|n|}=x^{-1}*x^{-1}*x^{-1}*\ldots*x^{-1}$.(n tane)

Ayrıca etkisiz elemanı da şu şekilde tanımlarız: $x^0=e$.

Herhangi bir (G,*) grubun en belirgin özelliği büyüklüğü yani grubun temelini oluşturan G kümesinin eleman sayısıdır. Buna (G,*) grubunun order'ı denir.

Tanım: (G,*) grubunun order'ı G kümesinin kardinalitesidir ve |G| şeklinde gösterilir.

Eğer bir grup, sonlu sayıda elemana sahipse sonlu grup, ve grubun order'i gruptaki eleman sayısıdır. Diğer durumda grup sonsuz gruptur.

Eğer bir grup aşağıdaki ilave koşulu sağlıyor ise **abealian** grup adı verilir.

(G_5) Komutatiflik. $\forall a,b \in G$ için, a*b = b*a dır.

Eğer *H* grubu G grubunun bir alt grubu ise |*H*| değeri |*G*| değerini böler. Böylece eğer *G* grubunun *düzeni* bir asal sayıysa *G*' nin tek alt grubu kendisidir. Bu durumda G grubu çarpmalı olarak yazılabilir.

Eğer *G* grubu çarpmalı olarak yazılabilirse ve $g \in G$ olmak üzere g sayısı *G* grubunun düzeni ise bu *g* sayısı $i \in N \cup \{\infty\}$ ve $g^i = 1$ şartını sağlayan en küçük *i* değeridir. Burada $\forall\, j, l \in Z$:

$$g^j = g^l \quad \Leftrightarrow \quad j \equiv l \mod ord(g)\text{' dir.}$$

Tablo 1.13'deki Cayley tablosu ile tanımlanmış grubu ele alalım:

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Tablo 1.13

Her bir elemanı n bir tamsayı olmak üzere a^n biçiminde yazabileceğimizden bu grup için $a^1=a$, $a^2=b$, $a^3=c$ ve $a^4=e$ 'dir. Verilen herhangi bir eleman için bu gösterim aynı değildir. Örneğin, $b=a^2=a^6=a^{-2}$ vs. yazabiliriz. Aslında kümenin her bir elemanını a' nın kuvvetleri biçiminde göstermek için sonsuz sayıda yol vardır. {e,a,b,c} 'nin her elemanı a^n biçiminde yazılabilir ve bu duruma a grubun bir üretecidir (generator) denir.

G grubunun alt grubu olan tüm gruplar *g* elemanının bir üssüdür ve <*g*> ifadesiyle gösterilirler. Eğer <*g*> = *G* ise *g* sayısı *G* grubunun **üreteci** (jeneratörü) olur. Bir üreteci olan tüm gruplara **devirli grup** (cyclic group) adı verilir.

G grubunun düzeni *p* asal sayısı ise grup içerisinde yer alan 1 dışındaki tüm sayılar *G* grubunun üreteci olur. Diğer bir deyişle <*g*> nin düzeni 1 veya *p* sayısı olur.

Doğal olarak, diğer başka elemanlar da grubun üretecimidir? sorusu aklımıza gelir. c elemanının

da bir üreteç olduğunu fakat n çift ise b^n=e ve b tek ise b^n=b olduğundan b ‘nin bir üreteç olmadığını söyleyebiliriz. En az bir tane üretece sahip gruplara halka denir.

Halkalar: {R,+,X) ile gösterilen bir *R* halkası, $\forall$a,b,c $\in$ R için aşağıdaki aksiyomları toplama ve çarpma ikili işlemleriyle sağlayan bir elemanlar kümesidir.

(G_1-G_5) R, toplama altında bir abelian grup tur.

(H_1) Çarpma altında kapalılık, Eğer a ve b $\in$ R ise ab$\in$ R dir.

(H_2) Çarpma ile birleşme özelliğine sahiptir. $\forall$a,b,c $\in$ R için, a(bc) = (ab)c dir.

(H_3) Dağılma kuralı, $\forall$a,b,c $\in$ R için, a(b+c) = ab + ac , (a+b)c = ac +bc dir.

Eğer bir halka aşağıdaki koşulu sağlıyor ise komutatif halkadır.

(G_4) Çarpmada Komutatiflik. $\forall$a,b $\in$ R için, ab = ba dır.

Eğer bir komutatif halka aşağıdaki aksiyomları sağlıyor ise integral domain dir.

(H_5) Çarpımsal etkisiz eleman. $\forall$a $\in$ R için, a1 = 1a =a dır.

(H_6) Sıfır bölen olmaması $\forall$a,b$\in$R ve ab=0 ise ya a=0 veya b=0 dır.

Alanlar(Field) : {F,+,X) ile gösterilen bir *F* alanı, $\forall$a,b,c $\in$ F için aşağıdaki aksiyomları toplama ve çarpma ikili işlemleriyle sağlayan bir elemanlar kümesidir.

(G_1-H_6) F, G_1 den G_5 ‘e ve H_1den H_6 ya aksiyomları sağlayan bir integral domain dir.

(H_7) Çarpımsal invers . $\forall$a $\in$ F için (sıfır hariç) F’de bir a^{-1} vardır ve aa^{-1}= (a^{-1})a =1dir.

Esasında bir **alan**, kümenin dışına çıkmaksızın, toplama çıkartma çarpma ve bölme yapılabilen bir kümedir. Bölme a/b = a(b^{-1}) kuralı ile tanımlanır.

1.8.2 Modüler Aritmetik

Modüler aritmetik “saat aritmetiğidir”

Tanım *a, r* ve *n* tam sayıları ve $n \neq 0$ şartı için, eğer *a* ve *b* nin farkı *n* ‘in *k* katı kadarsa bu şu şekilde gösterilebilir:

$$a = k \, . \, n \; + r$$

burada; a ve n pozitif tamsayılardır. Bu bağıntıyı sağlayan k ve r değerlerini her zaman bulmak mümkündür. kn’den a ya olan uzaklık r’dir ve kalan(residue) olarak adlandırılır. Veya eğer a ve n pozitif tamsayı iseler, a mod n , a ,n ile bölündüğünde kalan olarak tanımlanır. Böylece herhangi a tamsayısı için,

a= [a/n]x n + a ***mod*** n her zaman yazılabilir. (Örn: 11 mod 7 = 4)

a ve b iki tamsayısı eğer a ***mod*** n =b ***mod*** n iseler benzer modulo n olarak tanımlanır ve $a \equiv b$ mod *n* olarak yazılabilir.

Bölenler: Eğer sıfır olmayan bir b ve m tamsayısı için a=mb şeklinde yazılabiliyorsa b,

a’yı böler denir. Böyle bir bölünebilirlik var ise kalan sıfırdır. b|a notasyonu b’nin a’yı kalansız bölebildiğini belirtmek için sıkça kullanılır. Aşağıdaki bağıntılar vardır.

- Eğer a|1 ise a= ±1 dir.
- Eğer a|b ve b|a ise a= ±b dir.
- Herhangi bir b ≠ 0 sıfırı böler.
- Eğer, b|g ve b|h ise , b|(mg +nh) herhangi m ve n tamsayıları için vardır.

Teorem 1.34: a_1, a_2 ve n tam sayıları ve $n \neq 0$ şartı için,

$$(a_1 \; op \; a_2) \bmod n \equiv [(a_1 \bmod n) \; op \; (a_2 \bmod n)] \bmod n$$

denkliği gösterilebilir, burada *op*, “ + ” veya “ * ” şeklinde bir operatör olabilir.

- Bir `a = b mod n` eşitliği, a ve b aynı *n* ile bölündüğünde aynı kalanı verdiklerini ifade eder. Örnek,
  - `100 = 34 mod 11`
  - Genellikle `0<=b<=n-1` dir.
  - `2mod7 = 9mod7`
  - b ‘ye `a mod n ‘nin kalanı denir.`
- Tamsayı modulo n ile yapılan bütün aritmetikte bütün sonuçlar 0 ve n arasında olur.

Modül işleminin özellikleri

Modül işlemi aşağıdaki özelliklere sahiptir.

Eğer, n|(a-b) ise a ≡ b ***mod*** n dir.

a ≡ b ***mod*** n , b ≡ a ***mod*** n anlamına gelir.

a ≡ b ***mod*** n ve b ≡ c ***mod*** n , a ≡ c ***mod*** n anlamına gelir.

Modüler Aritmetik işlemleri

Toplama

`(a+b) mod n` = [(a mod n) + (b mod n)] mod n

Çıkartma

`(a-b) mod n` = [(a mod n) - (b mod n)] mod n

Çarpma

`axb mod n` = [(a mod n) x (b mod n)] mod n

- Tekrarlanan toplamdan türetilir
- Ne a ne de b sıfır değil iken `a.b=0` olabilir
  - örnek `2.5 mod 10`

Bölme

`a/b mod n`

- b nin tersi ile çarpmak gibidir: $a/b = a.b^{-1} \bmod n$
- eğer n asal ise $b^{-1} \bmod n$ vardır. $b.b^{-1} = 1 \bmod n$
  - örnek `2.3=1 mod 5` bu nedenle `4/2=4.3=2`

`mod 5` dir.

Özellikler :

n'den küçük olan pozitif tamsayıların kümesi Z_n aşağıdaki gibi tanımlansın.

$$Z_n = \{ 0,1,\ldots\ldots\ldots,(n-1)\}$$

Z_n kalanlar sınıfı olarak adlandırılır. Daha doğrusu, Z_n de her bir tamsayı bir kalan sınıfını temsil eder. [r] = { a : a bir tamsayı; öyleki ; a = r mod n dir.]

Z_n içersinde yapılacak modüler aritmetik işlemleri Tablo 1.14'deki özellikleri Z_n deki tamsayılar ile sağlar. Z_n çarpımsal etkisiz eleman ile birlikte değiştirilebilen bir halka oluşturur.

Aynı zamanda, indirgeme tamsayılar halkasından tamsayı modulo n 'lerin halkasına bir homomorfizm olduğu için, bir işlem ve sonra modulo n i indirgeyip indirgemeyeceği veya indirgedikten sonra yapacağı işlem seçilebilir.

- `a+/-b mod n = [a mod n +/- b mod n] mod n`
- (a.b) mod n =((a mod n).(b mod n)) mod n

Özellik	Açıklama
Değişme Kuralı (Commutative)	(a + b) mod n = (b + a) mod n (a x b) mod n = (b x a) mod n
Birleşme Kuralı (Associative)	[(a+b) +c] mod n = [a +(b + c)] mod n [(axb) x c] mod n = [a x(b x c)] mod n
Dağılma Kuralı (Distributive)	[ax(b + c)] mod n = [(axb) + (axc)] mod n
Etkisiz eleman (Identity element)	(0 + a) mod n = a mod n (1xa) mod n = a mod n
Toplamsal invers(-a)	$\forall a \in Z_n$ için ; bir b vardır öyleki ; a + b = 0 mod n dir.

Tablo 1.14.

- eğer n, p asal sayısı olmaya zorlanırsa bu form bir **Galois Field modulo p** ve **GF(p)** ile gösterilir ve bütün tamsayı aritmetiğindeki normal kurallar geçerlidir.

GF(p) (Galois Field) şeklindeki sonlu alanlar.

Birçok kriptografik algoritmada sonlu alanlar önemli bir rol oynarlar. Bir sonlu alanın düzen(order) ı bir p asal sayısının n. kuvveti(p^n) olarak gösterilmelidir. Burada n pozitif bir tamsayıdır. Düzeni p^n olan bir sonlu alan, genellikle GF(p^n) olarak yazılır. GF sonlu alanı ilk defa çalışan matematikçi olan Galoi'den gelmektedir. Özel durum olan n=1 için, sonlu alan GF(p) olarak yazılır.

Özel durum olarak GF(2^n) ve GF(3^n) verilebilir.

Düzeni p olan bir sonlu alan GF(p), {0,1,........,p-1} Z_p tamsayılar kümesinin modulo p aritmetik işlemleri ile birlikte tanımlanmasıdır.

Burada herbir elemanın bir çarpımsal tersi vardır ve çarpımsal invers olarak (w^{-1}) Çarpımsal invers . $\forall w \in Z_p$ için (sıfır hariç) Z_p'de bir z vardır ve w***x***z= 1mod p 'dir.

Çünkü , w, p ye göre asaldır. Eğer, Z_p nin elemanlarını w ile çarparsak, sonuçtaki kalanlar Z_p nin elemanlarının tamamının tekrarıdır. Böylece en az bir kalanın değeri 1'dir.Bu yüzden Z_p 'de en az bir eleman vardır öyleki, w ile çarpıldığında kalan 1'dir. Bu tamsayı w'nın çarpımsal tersi(w^-

^{1}) dir.

Tablo1.15'de GF(7) sonlu alanında Modulo 7 nin toplamsal ve çarpımsal tersleri gösterilmiştir.

w	-w	w^{-1}
0	0	-
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

Tablo 1.15 Modulo 7 için toplamsal ve çarpımsal tersler

Asal Sayılar

Bir p >1 sayısı ancak ve ancak bölenleri ±1 ve ±p ise asal sayıdır. Asal sayılar, Açık-anahtarlı kripto sistemlerinde büyük rol oynarlar. Asal sayılarda karşımıza çıkan önemli problemler, asal bir sayının oluşturulması ve bir sayının asal olup olmadığının test edilmesidir. Asal sayı oluşturma, verilmiş bir [r_1,r_2] tam sayılar aralığında asal sayı bulma işlemidir.

Herhangi bir a>1 tamsayısı tek bir şekilde aşağıdaki gibi ifade edilebilir.

$$a = p_1^{a_1} p_2^{a_2} .... p_t^{a_t}$$

burada $p_1,p_2,......,p_t$ asal sayılardır ve a_i tamsayıdır. (örn: $3600 = 2^4 \times 3^2 \times 5^2$)

Tanım: $a^{s-1} \equiv 1 \bmod s$ şartını ve $1< a< s$ şartını sağlayan s tam sayısına a tabanına göre **sanki asal** (pseudoprime) sayı denir**.**

Teorem 1.35: (Fermat teoremi) p bir asal sayı olsun. Her p ile bölünemeyen a pozitif tam **sayısı için,**

$$a^p \equiv a \bmod p \qquad \text{denkliği;}$$

ve p ile bölünmeyen her a tam sayısı için ise $a^{p-1} \equiv 1 \bmod p$. denkliği her zaman doğrudur:
İsp: Önceki bölümlerde açıklandığı üzere, eğer,Z_p nin elemanlarını{0,1,....,(p-1)} a , modulo p ile çarparsak, sonuçtaki kalanlar Z_p nin elemanlarının tamamının sekansıdır. Bundan başka, a x 0 = 0mod p dir. Bu yüzden (p-1) sayı, { $a$mod p, 2$a$modp, ...,(p-1)$a$mod p } ,dizisi {1,....,(p-1)} sayısı ile aynı düzendedir. Her iki kümenin sayılarını çarpıp mod p'sini alarak aşağıdaki bağıntı yazılabilir.

$$a \times 2a \times .... \times ((p-1)a) \equiv [(a \bmod p) \times (2a \bmod p) \times .... \times ((p-1)a \bmod p] \bmod p$$

$$\equiv [1 \times 2 \times ...... \times (p-1)] \bmod p$$

$$\equiv (p-1)! \bmod p$$

Fakat, $a \times 2a \times ...... \times ((p-1)a) = (p-1)! a^{p-1}$ dir

Bu yüzden, $(p-1)! a^{p-1} \equiv (p-1)! \bmod p$. dir. Burada (p-1)! 'i atabiliriz. Sonuçta:

$$a^{p-1} \equiv 1 \bmod p \quad \text{olduğu gösterilmiş olur.}$$

Örnek: a=7, p = 19 verilsin.

$7^2 = 49 \equiv 11 \bmod 19$

$7^4 = 121 \equiv 7 \bmod 19$

$7^8 = 49 \equiv 11 \bmod 19$

$7^{16} = 121 \equiv 7 \bmod 19$

$a^{p-1} = 7^{18} = 7^{16} \times 7^2 = 7 \times 11 \equiv 1 \bmod 19$

alternatif olarak $a^p \equiv a \bmod p$ olarak da yazılabilir.

Euler Totient fonksiyonu n tam sayısı için Euler Totient fonksiyonu $\phi(n)$, n den daha küçük olan ve n ile aralarında asal olan bütün pozitif tam sayıların sayısını verir.

p **asal ise** $\boldsymbol{\phi(p) = p\text{-}1}$ **dir.**

$n=p.q$ ve p, q asal sayılar ise $\phi(n) = \phi(.pq). = \phi(p).\phi(q) = (p-1).(q-1)$ dir.

$\phi(n) = \phi(.pq)$.olduğunu görmek için, Z_n 'deki kalanlar kümesinin [0, 1, ..., (pq-1)]. Olduğunu düşünelim. Kalanlar kümesindeki {p, 2p,.......,(q-1)p}, {q, 2q, ..., (p-1)q} ve 0 , n'e göre asal değildirler. Buna uygun olarak,

$\phi(n) = pq – [(q-1) + (p-1) +1]$

$= pq –(p+q) +1$

$= (p-1) \times (q-1)$

$= \phi(p).\phi(q)$

elde edilir. Tablo 1.16'da n = 30 'a kadar olan sayıların $\phi(n)$ değerleri gösterilmiştir

n	ϕ(n)	**n**	ϕ(n)	**n**	ϕ(n)
1	1	11	10	21	12
2	1	12	4	22	10
3	2	13	12	23	22
4	2	14	6	24	8
5	4	15	8	25	20
6	2	16	8	26	12
7	6	17	16	27	18
8	4	18	6	28	12
9	6	19	18	29	28
10	4	20	8	30	8

Tablo 1.16. 1-30 arası sayılar için $\phi(n)$ değerleri

Teorem 1.36: (Fermat teoremi) Eğer ***s*** bir asal sayı ve ***OBEB*(*a,s*)**=1 ise ***s***, ***a*** tabanına göre bir sanki asal (pseudo prime) sayıdır.

Tek Yönlü Fonksiyon

F: X ⟶ Y

$\boldsymbol{f}: \quad x \longrightarrow \quad f(x)=y$ yalnız ve yalnız aşağıdaki şartları taşıdığı takdirde tek yönlü bir fonksiyondur:

- $f(x)$ bütün x değerleri için polinomsal zamanda çözümlenebilir olmalıdır.
- Verilen bir y değeri için x değeri polinomsal zamanda bulunamamalıdır.

Örnek olarak verilirse $a^m \bmod n \equiv x$ bir modüler üs alma işlemidir ve kolaylıkla yapılabilir, fakat var olan x değerinden m değerini bulmak ayrık logaritma problemine girer ve

bunun da hesaplanma süresi polinomsal çözümleme süresinden çok daha uzundur.

Kapaklı Tek Yönlü Fonksiyonlar (Trapdoor One-Way Functions)

Kapaklı tek yönlü fonksiyonlarda ise tek yönlü fonksiyonlara ek olarak analizciye başka bilgiler verilirse fonksiyon daha kolay tersinir hale getirilebilir.

$y=f_k(x)$: eğer k ve x bilinirse y kolay hesaplanır.

$x=f^{-1}_k(y)$: eğer k ve y bilinirse x kolay, k bilinmezse zor hesaplanır.

Örneğin yalnız a^m mod n değerini bilmekten öte buradaki n değerinin iki asal sayının çarpımı olduğunu ve anahtarların bu sayılara bağlı olduğunu bilmek buradan m değerini bulma aşamasında analizciye ipucu vermiş olur.

1.9 Logaritma

Logaritma (Yunanca: λόγος (*logos*) = anlayış, ἀριθμός (*aritmos*) = sayı), 17. yüzyılın başında hesapları hızlandırmak için yapılan bir buluştur. 300 yıldan daha uzun bir zaman, temel bir hesap metodu olmuştur. 19. yüzyılda masa hesap makinalarının doğuşu ve yirminci yüzyılda elektronik hesap makinalarının ortaya çıkışı, logaritmaya olan ihtiyacı azaltmıştır. Ancak logaritmik fonksiyonların teorik ve uygulamalı matematikte özel bir yeri vardır.

Logaritma, birbirinden habersiz çalışan iki kişi tarafından keşfedilmiştir. Bunlar; 1614'te İskoçyalı John Napier ve 1620'de İsviçreli Joost Bürgi'dir.

Logaritma üzerinde önemli çalışmaları olan bir Türk bilgini de Gelenbevi İsmail Efendi'dir. Kendisi büyük bir matematikçi olup, mantıkla da uğraşmıştır. 1730-1790 yıllarında yaşayan bu büyük alimin *Logaritma Risalesi* isimli çok açık, anlaşılır yazılmış bir eseri mevcuttur.

Logaritma, tüm bilimlerde en faydalı aritmetik kavramlardan birisidir ve birçok bilimsel amaç için anlaşılması önemlidir. Logaritmayı çok farklı şekillerde tanımlamak mümkündür. Ancak burada en basit yöntem olan ve çarpma ve bölmenin toplama ve çıkarma işlemine indirgenmesine benzeyen yöntem seçilmiştir. Logaritmayı açıklamak için basit bir soru;

Matematikte, toplama işlemi performansında çarpma yapan bir işlem varmıdır?

Çok fazla düşünmeden sorunun cevabı aşağıdaki soru ile verilebilir.

2^3 x 2^4 'ün sonucu nedir? Sorusunun cevabı, her iki terimin de 2'nin kuvvetleri olması nedeniyle, üslerin toplanarak elde edilmesiyle 2^7 dir. Burada taban sayıların aynı olması gerekir.

Genel olarak, bu toplama $b^x x b^y = b^{x+y}$.olarak verilebilir Bu ifade herhangi iki sayının çarpılması işleminde kullanılabilir.(b^x olarak 1.3 ve b^y.olarak 6.9 diyebiliriz)

b tabanı olarak hangi sayıyı kullanabiliriz. Herhangi bir sayı kullanılabilse de genellikle on(=10) genel logaritma ve e(= 2.71828...), doğal logaritma kullanılır. Genel olarak $b^x= N$ ifadesinde N'nin b tabanına göre logaritması, x'tir.

Başka bir ifade ile, Logaritma, çıkarmanın toplama, çarpmanın bölme karşıtı olduğu gibi üs işleminin karşıtıdır.Teknik olarak söylenirse, log üs'ün tersi işlemdir. Pratik terimlerle, aşağıdaki eşdeğerlik söylenebilir.

$y = b^x$ ve $\log_b(y) =x$ eşdeğerdir (Aynı şeydir)

Yukarıdaki ifadenin sol tarafındaki üstel "$y = b^x$". ifadesi ve sağ tarafındaki "$\log_b(y) = x$" y'nin b tabanına göre logaritması x'ye eşittir şeklinde söylenen ifade eşdeğerdir. Burada b'ye taban denir ve her zaman pozitif ve 1'den büyüktür.

Tanım(matematiksel)

$b \in R^+ -\{1\}$ ve $x \in R^+$ olmak üzere, $b^y = x$ eşitliğini ele alırsak.

Bu eşitlikte; b değerini bulmak için **kök alma**, x değerini bulmak için **kuvvet (üs) alma** ,

y değerini bulmak içinde **logaritma** işlemi yapılır.

$b \in R^{+}-\{1\}$, $x \in R^{+}$ ve $y \in R$ olmak üzere,

$b^{y}=x \Leftrightarrow y=\log_{b} x$ tir.

Burada; y sayısı , x sayısının b tabanına göre logaritmasıdır.

Örnekler:

1) $\log_2 8 = y \Rightarrow 8= 2^{y} \Rightarrow y = 3$ tür.

2) $\log_a 64 = 3 \Rightarrow 64 = a^{3} \Rightarrow a = 4$ tür.

3) $\log_3 x = -2 \Rightarrow x = 3^{-2} \Rightarrow x = \frac{1}{9}$ dur.

4) $\log_a a = x \Rightarrow a = a^{x} \Rightarrow x = 1$ dir.

5) $\log_a 1 = n \Rightarrow 1 = a^{n} \Rightarrow n = 0$ dır.

6) $\log_5 (-25)$ v= $m \Rightarrow -25 = 5^{m} \Rightarrow m \notin R$ dir.

Sonuç olarak:

1) $\log_a a = 1$

2) $\log_a 1 = 0$

3)$y = \log_a f(x) \Rightarrow f(x) > 0$

Örnek:

$\text{Log}_5 (\log_3 (\log_2 x)) = 0$ olduğuna göre, x değerini bulalım.

Çözüm:

$\text{Log}_5 (\log_3 (\log_2 x)) = 0 \Rightarrow \log_3 (\log_2 x) = 5^{0} = 1 \Rightarrow \log_2 x = 3^{1} \Rightarrow x = 2^{3} = 8$ dir.

Örnek:

$\text{Log}_3 (a^{3}.b.c) = 5 \quad \log_3 \left(\frac{b^2}{c}\right) = 1$ olduğuna göre, a.b çarpımını bulalım.

Çözüm:

$\log_3(a^{3}.b.c) = 5 \Rightarrow$ a3.b.c $= 3^{5}$

$\log_3\left(\frac{b^2}{c}\right)=1 \quad \Rightarrow \quad \frac{b^2}{c}=3^{1}$

x

$a^{3}.b^{3} = 3^{6}$

$a.b = 3^{2}$

a.b = 9 dur.

Özel Logaritmalar

a) Bayağı Logaritma

$y = \log_{10} x = \log x$ fonksiyonuna **10 tabanında logaritma** veya **bayağı logaritma** denir.

Örnek: $\log_{10} 10 = \log 10 = 1$ dir.

b) Doğal Logaritma

e = 2,71828…. olmak üzere,

$y = \log_e x = \ln x$ fonksiyonuna **doğal logaritma** denir.

Örnek: $\text{Log}_e\, e = \ln e = 1$ dir.

Logaritmanın Özellikleri

$x,y \in R^+$ ve $b \in R^+ - \{1\}$ olmak üzere,

1) $\log_b (x.y) = \log_b x + \log_b y$

2) $\log_b \left(\frac{x}{y}\right) = \log_b x - \log_b y$

3) $\log_{b^n} x^m = \frac{m}{n} \log_b x$

4) $\log_b x = \log_b y \Rightarrow x = y$ dir.

Örnek:

1) $\log 5 + \log 2 = \log (5.2) = \log 10 = 1$

2) $\log 300 - \log 3 = \log \left(\frac{300}{3}\right) = \log 100 = \log (10^2) = 2.\log 10 = 2$

3) $\log_{25} 125 = \log_{5^2} 5^3 = \frac{3}{2} \log_5 5 = \frac{3}{2}$

Örnek:

$\log (2x-y) = \log x + \log y$ olduğuna göre, y nin x türünden eşitini bulalım.

Çözüm:

$\log (2x-y) = \log x + \log y \Rightarrow \log (2x-y) = \log (x.y)$

$\Rightarrow 2x - y = x.y$

$\Rightarrow 2x = x.y + y$

$\Rightarrow 2x = y.(x+1)$

$\Rightarrow y = \frac{2x}{x+1}$ dir.

Örnek: $\log (a.b) = 3$

$\log \left(\frac{a}{b}\right) = 1$ olduğuna göre, a değerini bulalım.

Çözüm:

$\log (a.b) = 3 \Rightarrow \log a + \log b = 3$

$\log\left(\frac{a}{b}\right) = 1 \Rightarrow \log a - \log b = 1$

+

$2 \log a = 4$, $\log a = 2$, $a = 10^2 = 100$ dür.

Örnek:

$\log_2 \sqrt{2.\sqrt[3]{2.\sqrt{2}}}$ işleminin sonucunu bulalım.

Çözüm:

$\log_2 \sqrt{2.\sqrt[3]{2.\sqrt{2}}} = \log_2 \sqrt[12]{2^6.2^2.2} = \log_2 \sqrt[12]{2^9} = \log_2 2^{\frac{3}{4}} = \frac{3}{4}$ tür.

Örnek:

log 5 = a, log 3 = b, log 2 = c olduğuna göre, log (22,5) ifadesinin a,b,c türünden eşitini bulalım.

Çözüm:

$\log (22,5) = \log \left(\frac{45}{2}\right) = \log \left(\frac{5.3^2}{2}\right) = \log 5 + \log 3^2 - \log 2 = \log 5 + 2\log 3 - \log 2$

$= a + 2b - c$ dir.

Örnek:

$\text{Log}_5\, x^2 = 6 + \log_5 \frac{1}{x}$ olduğuna göre, x değerini bulalım.

Çözüm:

$\text{Log}_5\, x^2 = 6 + \log_5 \frac{1}{x} \Rightarrow 2.\log_5 x = 6 + \log_5 x^{-1}$

$\Rightarrow 2.\log_5 x = 6 - \log_5 x$

$\Rightarrow 3.\log_5 x = 6$

$\Rightarrow \log_5 x = 2$

$\Rightarrow x = 5^2 = 25$ tir.

Örnek:

log 5 = n olduğuna göre, log 4 değerinin n türünden eşitini bulalım.

Çözüm:

$\log 4 = 2 \log 2 = 2 \log \frac{10}{5} = 2.(\log 10 - \log 5) = 2(1-n)$ dir.

$a \in R^+$, $a \neq 1$ ve $x \in R^+$ olmak üzere,

$a^{\log_a x} = x$ tir. $a^{\log_b c} = c^{\log_b a}$ dır.

Örnek:

$3^{\log_3 5} = 5$, $e^{\ln 3} = 3$ ve $10^{\log A} = A$ dır.

Örnek:

$9^{\log_3 10} = 10^{\log_3 9} = 10^{2.\log_3 3} = 10^2 = 100$ dür.

Taban Değiştirme Kuralı:

$a \neq 1, b \neq 1$ ve $a,b,c \in R^+$ olmak üzere,

$$\log_a c = \frac{\log_b c}{\log_b a} = \frac{\log c}{\log a} = \frac{\ln c}{\ln a}$$ dır.

Not:

$a \neq 1, b \neq 1$ ve $a,b \in R^+$ olmak üzere,

$$\log_a b = \frac{1}{\log_b a}, \ \log x = \frac{1}{\log_x 10}$$ olur.

Örnek:

$\log_2 5 = x$ olduğuna göre, $\log_5 10$ ifadesinin x türünden eşitini bulalım.

Çözüm:

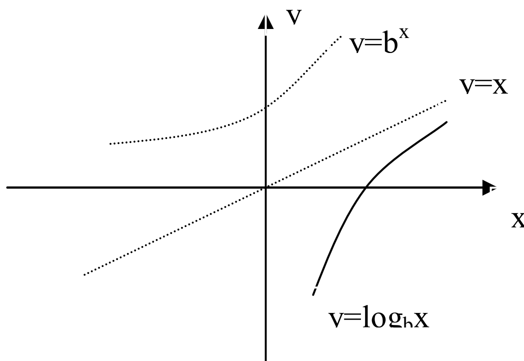
$$\log_5 10 = \frac{\log_2 10}{\log_2 5} = \frac{\log_2 2 + \log_2 5}{\log_2 5} = \frac{1+x}{x}$$ olur.

Logaritma Fonksiyonunun Grafiği

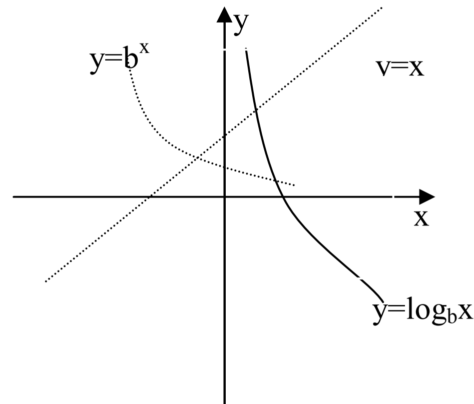
Üstel fonksiyon bire bir ve örten olduğu için ters fonksiyonu vardır ve bu fonksiyona **logaritma fonksiyonu** denir.

Y = $\log_b$ x fonksiyonunun grafiği b nin durumuna göre çizilirse, Şekil 1.18 ve 1.19 daki grafikler elde edilir.

1. b>1 için 2. 0<b<1 için



Şekil 1.18



Şekil 1.19

Not: y =f(x)= $\log_b$ (mx + n)fonksiyonunun grafiği, aşağıdaki işlemler yapılarak çizilir.

1) Logaritmanın tanımından, f(x) in grafiği, mx + n > 0 şartının sağlandığı bölgededir.

2) y = 0 ve y = 1 için sırasıyla x_0 ve x_1 değerleri bulunur. Grafik, $(x_0,0)$ ve $(x_1,1)$ noktalarından geçer.

Örnek: f(x) = $\log_2$ (x-1) fonksiyonunun grafiğini çizelim.

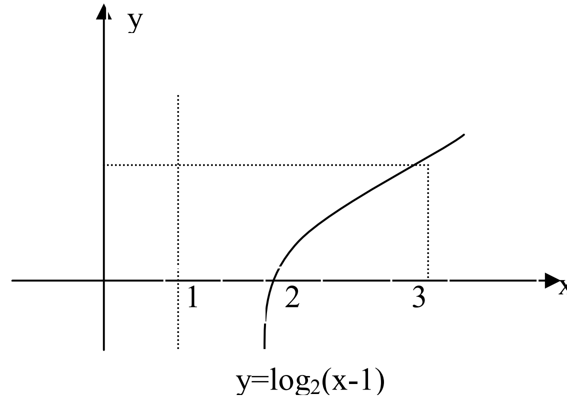
Çözüm:

f(x) fonksiyonu, x-1>0 $\Rightarrow$ x>1 için tanımlıdır.

y = 0 için, $\log_2 (x-1) = 0 \Rightarrow x = 2$ ve

y = 1 için, log2 (x-1) = 1 $\Rightarrow$ x = 3

olduğundan grafik (2,0) ve (3,1) noktalarından geçer. Taban 1 den büyük olduğundan, verilen fonksiyonun grafiği,



$y=\log_2(x-1)$

Şekil 1.20

Logaritma Fonksiyonunun tersi

$b \in R^+ - \{1\}$ ve $x \in R^+$ olmak üzere,

$f(x) = \log_b x \Leftrightarrow f^{-1}(x) = b^x$ tir.

Örnek:

$f(x) = \log_5 x \Leftrightarrow f^{-1}(x) = 5^x$ tir.

Örnek:

$f(x) = y = 2\log_5 x \Rightarrow x = 2.\log_5 f^{-1}(x)$

$\frac{x}{2} = \log_5 .f^{-1}(x) \Rightarrow 5^{\frac{x}{2}} = f^{-1}(x)$

$\Rightarrow f^{-1}(x) = \left(\sqrt{5}\right)^x$ tir.

Logaritmalı Eşitsizlikler

Bir eşitsizlik içinde bilinmeyenin logaritması varsa bu tür eşitsizliklere **logaritmalı eşitsizlikler** denir.

1) b>1 olmak üzere,

$\text{Log}_b f(x) \geq \log_b g(x) \Leftrightarrow f(x) \geq g(x)$ (eşitsizliğin yönü değiştirilmez.)

2) 0<b<1 olmak üzere,

$\text{Log}_b f(x) \geq \log_b g(x) \Leftrightarrow f(x) \leq g(x)$ (eşitsizliğin yönü değiştirilir.)

Örnek:

$\log_3 (\log_2(x-1)) > 0 \Rightarrow \log_2 (x-1) > 3^0 = 1$

$\Rightarrow x-1 > 2^1$

$\Rightarrow x > 3$ tür.

Örnek:

$\log_2(x-3)<4 \Rightarrow 0 < x-3 < 2^4$

$\Rightarrow 3<x<19$ dur.

Örnek:

$\log_{\frac{1}{2}}(3x-1) < 0 \Rightarrow \log_{2^{-1}}(3x-1) < 0$

$\Rightarrow -\log_2(3x-1) < 0$

$\Rightarrow \log 2\,(3x-1) > 0$

$\Rightarrow 3x-1 > 1$

$\Rightarrow x > 2/3$' tür.

Bayağı Logaritma

a) Karakteristik ve Mantis

$x \in R+$, $k \in Z$ ve $0 \leq m < 1$ olmak üzere, **log x = k+m** eşitliğinde k tamsayısına x in **logaritmasının karakteristiği**, m reel sayısına da x in **logaritmasının mantisi** denir.

Örnek:

log 30 = 1,477 ifadesinde, 30 sayısının logaritmasının karekteristiği1 ve mantisi 0,477 dir.

Örnek:

log2 = 0,301 olduğuna göre, log(800) değerinin karakteristik ve mantisini bulalım.

Çözüm:

$\log(800) = \log(2^3.10^2) = 2 + 3\log 2$

$= 2 + 3.(0{,}301)$

$= 2 + 0{,}903$

$= 2{,}903$ olduğundan,

karakteristik 2 ve mantis 0,903 olur.

Not:

$\bar{4}.046 = -4 + 0{,}046$ ve

$\bar{4}{,}046 \neq -4{,}046$ olduğuna dikkat edilmelidir.

Uyarı:

1 den büyük pozitif tamsayıların basamak sayısı, sayının logaritmasının karakteristiğinin bir fazlasıdır.

Örnek:

log 2 = 0,301 olduğuna göre, $(40)^{40}$ sayısının kaç basamaklı bir sayı olduğunu bulalım.

Çözüm:

$\text{Log}\,(40)^{40} = 40.\log(40)$

$= 40.(\log 2^2.10)$

$= 40.(1 + 2\log 2)$

$= 40.(1 + 0{,}602) = 64{,}08$ olduğundan, karakteristik 64 ve basamak sayısı 65 tir.

b) Kologaritma:

$x \in R^+$ olmak üzere, x in çarpmaya göre tersinin logaritmasına x in kologaritması denir ve colog x biçiminde gösterilir.

$\text{Colog}\,x = \log \frac{1}{x} = \log x^{-1} = -\log x$ tir.

Örnek:

$\log x = 1{,}73$ olduğuna göre, colog x in karakteristiğini ve mantisini bulalım.

Çözüm:

$\log x = 1{,}73 \Rightarrow \text{colog } x = -\log x = -1{,}73 = -2 + 0{,}27 = \bar{2}{,}27$ dir.

colog x in karakteristiği –2 ve mantisi 0,27 dir.

Örnek:

$\log A = \bar{3}{,}52$ olduğuna göre , colog A değerini bulalım.

Çözüm:

$\log A = \bar{3}{,}52 \Rightarrow \text{colog } A = -(\bar{3}{,}52)$

$= -(-3 + 0{,}52)$

$= 3 - 0{,}52$

$= 2{,}48$ dir.

1.10 Olasılık

Olasılık kuramı rastgele olayların analizi ile ilgilenen bir matematik bilim dalıdır. Olasılık kuramının ana öğeleri rassal değişkenler, saf rassal süreçler, olaylar olarak sayılabilir. Bunlar ya tek olarak ortaya çıkan veya bir zaman dönemi içinde gelişerek meydana gelen, ilk görünüşü rastgele bir şekilde olan deterministik olmayan olayların veya ölçülebilir miktarların matematiksel soyutlamalarıdır. Bir madeni parayı yazı-tura denemesi için havaya atmak, veya bir zarı atmak ile ortaya çıkan sonuç ilk bakışta rastgele bir olay olarak görülebilirse bile eğer birbirini takip eden rastgele olaylar tekrar tekrar ortaya çıkartılırsa, incelenebilecek ve tahmin edilebilecek belirli bir istatistiksel seyir takip ettikleri görülecektir. Bu türlü olaylar ve sonuçların seyirlerini betimleyen iki temsilci matematiksel sonuç büyük sayılar yasası ve merkezsel limit teoremidir.

İstatistik bilim dalının matematiksel temelini oluşturan **olasılık kuramı**, büyük veri serilerinin niceliksel analizini gerektiren birçok insan faaliyetinin incelenebilmesi ve anlanabilmesi için temel esasları oluşturur. Bunun yanında, **olasılık kuramı**nın yöntemleri, durumları hakkında sadece kısımsal bilgimiz olabilecek karmaşık sistemlerin tanımlanmasına da uygulanabilir; (örneğin istatistiksel mekanik). Yirminci yüzyılda fizik biliminde en büyük buluşlardan biri, atomik düzeyde fiziksel olayların tabiatının olasılıklı olduğu ve bunların kuantum mekanik bilgisi ile açıklanıp, incelenip, kullanılabileceğidir.

Tarihçe

Matematiksel olasılık kuramının tarihsel kökleri 16. yüzyılda Gerolamo Cardano ve 17. yüzyılda Pierre de Fermat ile Blaise Pascal tarafından yapılan şans oyunlarının matematiksel incelemelerine dayanır.

Başlangıçta, olasılık kuramı genellikle *ayrık* olayları incelemek için geliştirilmiş ve kullanılan yöntemler genellikle tümleşik matematik kurallarına dayandırılmıştır. Fakat giderek matematik analiz görüşleri daha ağır basarak olasılık kuramına *sürekli* değişkenlerin incelenmesinin de katılması gerekmiştir. Bu gelişmenin şu andaki en son aşamasının temelleri, Andrey Nikolaevich Kolmogorov tarafından, ölçüm kuramına bağlantılı olan modern olasılık kuramı olarak ortaya çıkartılmıştır. Kolmogorov, Richard von Mises tarafından ortaya atılan **örneklem uzayı** kavramlarını **ölçüm kuramı** kavramları ile birleştirerek 1933de modern olasılık kuramı için esas olan Kolmogorov aksiyomlarını ortaya atmıştır. Bu gelişme bilim camiası tarafından çabucak, hiç karşı çıkan kuram olmadan, modern olasılık kuramının ana aksiyom sistemi olarak benimsenmiştir.

Belli olasılıklarla değişik değerler alabilen değişken **rastsal değişken** olarak adlandırılır. Bir zar atıldığında elde edilen 1,2,3,4,5 ve 6 sonuçları **x** rastsal değişkeninin değerleridir. Bu sonuçlardan her biri 1/6 olasılığı ile ortaya çıkar. Stokastik değişken olarak da adlandırılan rastsal değişken süreklilik açısından ikiye ayrılır :

- Ayrık tipte rastsal değişken
- Sürekli tipte rastsal değişken

Ancak Burada ağırlıklı olarak ayrık olasılık teorisi üzerinde durulacaktır.

1.10.1 Ayrık tipte rastsal değişken ve olasılık dağılımı

x rastsal değişkeninin 0,1,2,..... gibi sonlu veya sayılabilir sonsuzlukta tam değerler aldığı durumdur. Ailedeki çocuk sayısı, üretimdeki kusurlu mal sayısı gibi, ayrık tipte bir x değişkeni $x_1, x_2, ..., x_n$ değerleri alabilir.Ayrık tipte rastsal değişkenin olasılık dağılımı, olasılık fonksiyonu adı verilen bir fonksiyonla yada her x değerine karşı gelen olasılıkları gösteren bir tablo ile gösterilir. Ayrık tipte bir **x** rastgele değişkeni için verilen olasılık **P(x)** veya **f(x)** ile gösterilir.

$$f(x) = P(x)$$

ancak f(x)'in aşağıdaki koşulları sağlaması gerekir:
x=0,1,2,....n olmak üzere;

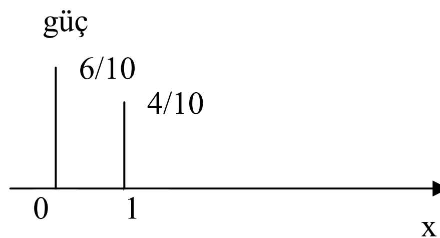
- $\Sigma f(x) = 1$ (bütün x 'ler için olasılıkların toplamı 1'dir.)
- $f(x) \geq 0$ (olasılıklar P(x) negatif olamaz)

Ayrık olasılık dağılımına örnekler: ayrık tekdüze dağılım, Bernoulli dağılımı, binom dağılımı, Poisson dağılımı,geometrik dağılım ,hipergeometrik dağılım

Örnek: bir kutuda aşağıda verilen iskambil kâğıtları bulunmaktadır:

kupa 2, 3, 4
maça 1, 2
sinek 3, 4
karo 1, 2, 3

Kutudan rastgele bir kâğıt çekersek x rastgele değişkeni çekilen siyah kâğıt sayısını göstermek üzere olasılık dağılımı ne olacaktır ?
Kutudaki toplam 10 kâğıdın 4'ü siyah olduğu için çekilen kâğıdın siyah olma olasılığı:
f(1) = P(x = 1) = 4 / 10
kırmızı kâğıt çekme olasılığı:
f(0) = P(x = 0) = 6 / 10
şekil olarak gösterirsek;



Şekil 1.21

1. Kutudan rastgele bir kâğıt çekersek ve **x** ile kâğıdın üzerindeki sayıyı gösterirsek, **x** 1,2,3,4 değerlerini alabilir. Bunların olasılıkları:
   f(1) = P(x = 1) = 2 / 10 (2 as)
   f(2) = P(x = 2) = 3 / 10 (3 adet ikili)
   f(3) = P(x = 3) = 3 / 10 (3 adet üçlü)
   f(4) = P(x = 4) = 2 / 10 (2 adet dörtlü)
2. iadeli olarak iki kâğıt çektiğimizde x siyah kâğıt sayısını göstermek üzere olasılık dağılımı nasıl olacaktır ? **K (** kırmızı) , **S** (siyah)
   İki kâğıt çekildiğinde sonuçlar:
   KK , KS , SK , SS olacaktır. Olaylar bağımsız olduğundan olasılıklar K ve S olaylarının olasılıkları çarpımı ile hesaplanacaktır.
   P(x = 0) = P(KK) = 6/10 * 6/10 = 9/25
   P(x = 1) = P(KS) = 6/10 * 4/10 = 6/25
   P(x = 1) = P(SK) = 4/10 * 6/10 = 6/25

P(x = 2) = P(SS) = 4/10 * 4/10 = 4/25

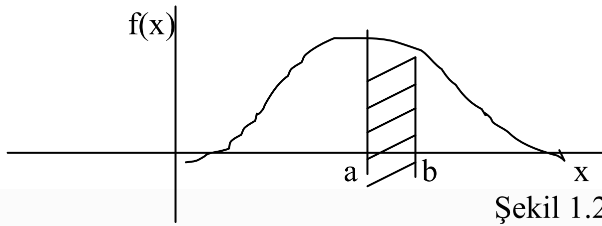
Örnek: 2 zarla atış yapıldığında x rastsal değişkeni zarların üste gelen yüzlerindeki sayıların toplamını gösterirse, şıklar 2 ve 12 arasında olacaktır. Olasılıklar şu şekildedir:

x(şıklar)	2	3	4	5	6	7	8	9	10	11	12
P(x)	1/36	2/36	3/36	4 /36	5/ 36	6/36	5/36	4/36	3/36	2/36	1/36

Sürekli rastsal değişken ve sürekli olasılık dağılımları

Sınırsız sayıda değer alabilen değişken sürekli rastsal değişken olarak adlandırılır. Bir sınıftaki öğrencilerin boy uzunluğu, belli bir marka ampulün dayanma süresi gibi ölçülebilen değişkenler sürekli rastsal değişkenlerdir. Herhangi bir **f(x)** fonksiyonunun sürekli bir rastsal **x** değişkeni için olasılık yoğunluk fonksiyonu olarak adlandırılabilmesi şu koşullara bağlıdır. Fonksiyonun integralinin alınabilmesi, alt ve üst sınırlarının -∞' dan + ∞'a kadar değişebilmesi ve

$f(x) \geq 0$ $\qquad \int_{-\infty}^{+\infty} f(x)*dx = 1$ olması gerekir



Şekil 1.22

Sürekli olasılık dağılımına örnekler: sürekli tekdüze dağılım,normal dağılım,Student'in t dağılımı,F-dağılımı ,ki-kare dağılımı,üstel dağılım,beta dağılımı ,gamma dağılımı

Temel Prensipler:

Belirli bir olay A için olasılık P(A) 0 ile 1 arasında değişen bir sayı ile temsil edilir. Hiç olanaksız bir olay için olasılık 0 olur ve kesinlikle olacak bir olayın olasılığı 1 olur. Bazı istatistikçiler bu uçsal olasılık değerlerinin sadece teorik olduğunu iddia etmektedirler çünkü kabul ettikleri olasılık açıklaması deneylemelerle limitte göresel çokluluk (relatif frekans) değerine dayanır. Diğer Bayes-tipi, özellikle subjektif, olasılık açıklamasına göre bu uçsal olasılık değerlerini sübjektif olarak düşünmek ve olaylara bu değerleri koymak imkân dahilindedir.

Olasılığın incelenmesinde sonucu bilinemeyen deneyler göz önüne alınacaktır. Bu deneylerin birçoğu tekrar edilebilir deneylerdir ve rastgele deneyler(random experiment) olarak adlandırılır. Her deneyin sonucu gözlenebilir ve liste olarak yazılabilir.Madeni para veya zar ile atış yapmak, üretilen makine parçaları arasından kusurlu olanları belirlemek, bir ana kitle içinden örnek seçmek tekrarlanabilir deneylerdir. Madeni para ile iki defa atış yapalım.Bu iki atımda 4 durumdan biri ortaya çıkacaktır.
Y ile yazı , T ile tura gösterilmek üzere;

YY YT TY TT

Deneylerin sonuçları **olay** olarak tanımlanmaktadır. Zar ile yapılan atışta olaylarımız veya sonuçlarımız 1,2,3,4,5 ve 6 nın üste gelmesi olacaktır. Bu sonuçların her biri birer basit olaydır. Özetle **basit olay** tek bir deneyde tek bir sonuç veren olaylardır**. P(E)** ile basit olayın gerçekleşme olasılığı gösterilir. Madeni para ile tek atışta tura gelmesi basit olaya örnek olarak verilebilir.Bir deneyin bütün sonuçları o deneyin örnek uzayını meydana getirir.Örnek uzay **S** harfi ile gösterilir.
Bir deneyin olası sonuçlarından herbirini **E** ve örnek uzayı **S** ile gösterirsek bir zarın atılışında örnek uzay;

S= {E_1 , E_2, ...,E_6 } şeklindedir.
Örnek :Bir lotarya oyununda üç basamaklı bir tam sayı rastgele seçilmektedir.Üç basamaklı sayıların herbiri olası bir sonuçdur.Örnek uzay;
S = { 000,001,002,.........,998,999 }
Örnek:Bir kutuda siyah ve sarı renk de toplar bulunmaktadır.Kutudan bir top çekip tekrar yerine koyarsak ve bu deneyi 100 defa tekrarlarsak çekilen topun sarı ya da siyah olması gerektiğinden deneyin 2 basit olayı olacaktır.
E_1 =siyah topun çekilmesi,
E_2 =sarı topun çekilmesi,
örnek uzay S = {E_1 , E_2 }
İki veya daha çok olayın birlikte veya birbiri ardına gerçekleşmesi ile bileşik olay meydana gelir. Bileşik olayın gerçekleşme olasılığı E_1 , E_2 iki olayı göstermek üzere **P(E_1 , E_2)**şeklindedir.
Para ile iki atış yapıldığında;

YY YT TY TT

Sonuçlarının çıkması bir bileşik olaydır.Aynı şekilde zarla yapılan 2 atışta 6*6=36 sonucu da bileşik olaydır. Basit ve bileşik olay tanımlarından başka olayı **bağımlı** ve **bağımsız** olay olarak da tanımlayabiliriz. Bir olayın ortaya çıkması diğer bir olayın veya olayların ortaya çıkmasına neden olmuyorsa bu olaylar **bağımsız** olaylardır. Zarın 2 defa atılmasında 1. atışın sonucu, 2.atışı etkilemeyeceği için bağımsız olay olarak adlandırılır. Bir olayın meydana gelmesi diğer bir olayın veya olayların meydana gelmesini etkiliyorsa bu tür olaylar **bağımlı** olaylardır. 52'lik iskambil destesinden iadesiz olarak arka arkaya 2 kâğıt çekildiğinde, ikinci kartın sonucu birinci kartın sonucuna bağımlıdır.
Sonlu Olasılık
Bir olay mümkün olan ve ortaya çıkma şansı eşit olan tüm durumlardan(S), sadece (E) kadar ortaya çıkıyorsa o olayın olasılığı ;

$$P(E) = |E| / |S| \text{ dir.}$$

Bir başka deyişle bir olayın ortaya çıkış sayısı toplam haller sayısına bölündüğünde elde edilen oran o olayın olasılığıdır.
Örnek: Bir zarın bir kere atılışı deneyinde her olayın olasılığı 1 / 6 dır. Örnek uzay ise;

$$S = \{1, 2,3,4,5,6 \}$$

2 veya 5'in üste gelmesi olayını E ile gösterirsek;
E = { 2,5 } P(E) = 1/6 + 1/6 =2/6 = 1/3
E'nın ortaya çıkmama olasılığını(1,3,4 veya 6'nın üste gelmesi) E' ile gösterirsek;
P(E') = 1/6 + 1/6 + 1/6 + 1/6 = 4 / 6 = 2/ 3 veya
P(E') = 1- P(E) = 1 – 1/ 3 = 2 / 3
Örnekten anlaşılacağı gibi bir olayın olasılığı 0 ve 1 arasında değişmektedir. Olayın ortaya çıkması mümkün değilse olasılığı 0, ortaya çıkması muhakkak ise olasılığı 1 dir. Eğer bir olayın meydana gelme olasılığı p ve gelmeme olasılığı q ise, olayın gerçekleşme olasılığının oranı (g**erçekleşme şansı**) p/q, gerçekleşmeme olasılığının oranı q / p dir.
Örneğin zar atıldığında 3 veya 4 gelmemesi şansı (2 / 3) / (1 / 3) = 2 /1 dir.

Olasılıkları belirlemek

Sonlu veya sayılabilir miktardaki sonuç bulunan deneylerin örnek uzayı S verilsin. Her bir sonuç için p(s) olasılığı belirlenirse; iki koşul gerekli olacaktır.
i) $0 \leq p(s) \leq 1$
ii) $\sum_{s \in S} p(s) = 1$

Koşul i her bir sonucun olasılığının pozitif ve bire eşit veya küçük, koşul ii ise bütün olayların sonuçlarının olasılığı toplamının bire eşit olduğunu ifade eder.

Tanım: E olayının olasılığı E'deki sonuçların olasılıklarının toplamına eşittir ve aşağıdaki şekilde gösterilir. P(E) = $\sum_{s \in S} p(s)$

Örnek: Bir oyun zarı öyle yüklenmiştir ki, 3 iki tane, diğer sayılar ise eşit olarak beş tane bulunur. Bu zarı yuvarladığımızda tek sayı çıkma olasılığı nedir?

Çözüm: E ={ 1,3,5} sayılarının gelme olasılığını bulacağız.

Burada p(1)= p(2)= p(4)= p(5)= p(6)= 1/7, p(3)= 2/7 dir.

Toplam olasılık p(E) = p(1) + p(3)+ p(5) = 1/7 +2/7 + 1/7 = 4/7 dir.

Tanım: Bir S örnek uzayında E olayı verilsin. E nin tamamlayıcısı olan $\overline{E}$ 'nin olasılığı P($\overline{E}$) = 1-P(E) ile hesaplanır .

Burada |$\overline{E}$ | = |S|-|E| dir. P($\overline{E}$) = |$\overline{E}$ |/|S| = (|S|-|$\overline{E}$ |)/|S|= 1-P(E) dir. .

$\sum_{s \in S} p(s) = 1$= P(E) +P($\overline{E}$) dir.

Bileşik bir olayın ortaya çıkma olasılığı o olayı meydana getiren basit olayların olasılıkları toplamına eşittir. 2 zarın birlikte atılışında toplam 4 gelme olasılığı P(E), 1-3,3-1 ve 2-2 basit olayların olasılıkları toplamına eşittir:

P(E) = 1/ 36 + 1 / 36 + 1 / 36 = 1/ 12

Bileşik olayların birbirlerini engelleyip engellememelerine göre olasılıklar değişecektir. Örneğin bir deste iskambil kâğıdından bir defada bir as çekme (A) ve bir papaz çekme(B) olayları birbirini engeller. Bir defada hem as hem de papaz çekme olasılığı sıfırdır.

P(A , B) = 0

A ve B birbirini engelleyen olaylar olduğundan A olayının veya B olayının ortaya çıkması bu olayların basit olasılıklarının toplamına eşittir. (A+B) ile as veya papaz çekme olayını gösterirsek;

P(A+B) = P(A) + P(B) = 1/13 + 1/ 13 = 2/ 13

P(A veya B) = P(A) + P(B)

Benzer şekilde 2 zarın bir arada atılışında toplam 5 gelme olasılığı 4 basit olayın olasılıkları toplamına eşittir. (2-3),(3-2),(4-1),(1-4)

P(A)=P(2-3)+P(3-2)+P(1-4)+P(4-1) = 1 / 36 + 1 / 36 + 1 / 36 + 1 / 36= 4 / 36

Buradan şu sonuç çıkmaktadır. Birbirlerini engelleyen olayların olasılıkları toplamı 1 dir. Eğer olaylar birbirini engellemiyorsa A olayının veya B olayının ortaya çıkması, ya A olayının ya B olayının ya da A ve B olaylarının her ikisinin birlikte gerçekleşmesi anlamındadır. A ve B birbirlerini engellemiyorsa;

P(A+B)=P(A) + P(B) – P(AB)

veya P(A veya B)=P(A) + P(B) – P(A ve B)

örnek: bir deste iskambil kâğıdından bir vale çekme olayı A ile, bir maça çekme olayı da B ile gösterilsin. Bu iki olay birbirini engellemediğinden **A ve B** (AB) nin olma olasılığı yani maça valesi çekme olasılığı vardır. Bu durumda A'nın veya B'nin olma olasılığı;

P(A+B)=(4/52) + (13/52)-(1/52)=4/13

Koşullu olasılık

Bağımlı olaylardan birinin(**A**) gerçekleştiği bilindiğinde diğerinin (**B**) ona bağlı olarak meydana gelme olasılığı;

P(B | A) =P(A B) / P(A)

Örnek: bilgisayar müh. bölümü 1.sınıf öğrencilerinin %25'i matematik dersinde, %15'i de hem matematik hem fizik dersinde üstün başarı göstermiştir. Bu sınıftan rastgele bir öğrenci seçildiğinde, seçilen öğrenci matematik dersinden üstün başarılı ise, fizik dersinden de üstün başarılı olma olasılığı nedir ?

P(mat) = 0.25

P(mat ve fizik) = 0.15

P(fizik \ mat)=P(mat ve fizik) / P(mat) =0.15 / 0.25=0.60

Çarpma kuralı(bağımlı olay)

Bağımlı iki olaydan **B** olayı **A** olayından sonra ortaya çıkıyorsa, olayların birlikte gerçekleşme olasılığı;

P(A ve B) =P(A) * P(B|A)

Örnek: bir piyangoda 8 boş, 2 ikramiyeli bilet vardır. Bu piyangodan 2 bilet alan bir kişinin ikramiye kazanma olasılığı nedir ?

Birinci biletin kazanma olasılığı 2/10'dur.birinci bilet ikramiye kazanırsa geriye 8 boş 1 ikramiyeli 9 bilet kalır. İkinci biletin kazanma olasılığı 1/9'dur. Her iki biletin de ikramiye kazanma olasılığı;

$P(B_1 \text{ve } B_2)= (2/10)*(1/9) = 1/45$

Örnek: Bir kutuda 5 adet yeşil renkte, 3 adet de beyaz renkte top bulunmaktadır. Kutudan 2 top çekildiğinde her ikisinin yeşil olma olasılığı nedir ? (toplar kutuya iade edilmiyor)

A ile ilk çekilen topun yeşil olması olayı,

B ile ikinci çekilen topun yeşil olması olayı gösterilsin.

A ve B bağlı olaylar olduğu için P(A ve B) yani P(AB) hesaplanacaktır. 1. topun yeşil olma olasılığı :

P(A) = (5 / 8)

1. topun yeşil olması durumunda 2. topun yeşil olma olasılığı:

P(B | A) = (4 / 7)

P(A ve B) = P(A) * P(B | A) = (5/8)*(4/7) = 0.357

Çarpma kuralı(bağımsız olay)

Bağımsız olaylarda çarpma kuralı;

P(A ve B)= P(A) * P(B) şeklindedir. Aynı anda atılan iki zarın üzerinde 2 olması olasılığı;

P(2 ve 2)= P(1/6) * P(1/6) = 1/36

Örnek: A'nın 15 yıl sonra hayatta kalma olasılığı %80, B'nin 15 yıl sonra hayatta kalma olasılığı %60 ise, her ikisinin 15 yıl sonra hayatta kalma olasılığı nedir?

P(A ve B)=0.80 * 0.60 = 0.48

Örnek: Aşağıdaki tablonun verilerinden yararlanarak bazı olasılıkları hesaplamaya çalışalım:

	20 yaş	21 yaş	Toplam
Kız	18	12	30
Erkek	32	38	70
Toplam	50	50	100

Bu grup içinden seçilecek bir öğrencinin kız olma olasılığı: P(Kız) =30 / 100 = 0.30

Erkek olma olasılığı: P(Erkek) = 70 / 100 =0.70

20 yaşında olma olasılığı : P(20) = 50 / 100 = 0.50

Şimdi de bileşik olasılıkları hesaplayalım:

P(Kız ve 20 yaş) = 18 / 100 = 0.18

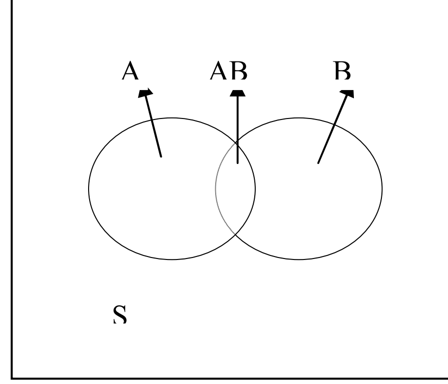
P(Erkek ve 21 yaş) = 38 / 100 = 0.38

Bir öğrencinin kız veya 20 yaşında olma olasılığı da:

P(Kız veya 20 yaş)= (30/100) + (50/100) – (18/100) = 62 / 100 = 0.62

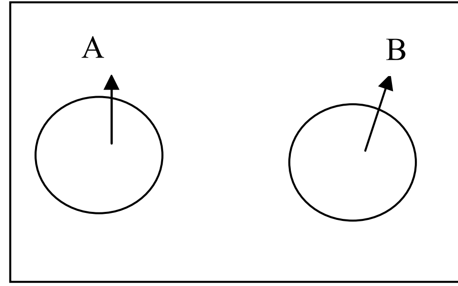
Olasılıkla ilgili bu hesaplamalar kümelerle de ifade edilebilir. Bir deneyin sonuçlarını veya basit olaylarını bir örnek uzayı içinde noktalar olarak belirtebiliriz. Basit olaylar noktalarla gösterilebilirler ancak bunların toplamı olan bileşik olaylar bir küme veya noktalar grubu olarak

gösterilirler. A ve B gibi birbirini engellemeyen iki bileşik olay ***Venn*** diyagramı ile Ş.1.23 deki gibi çizilebilir:



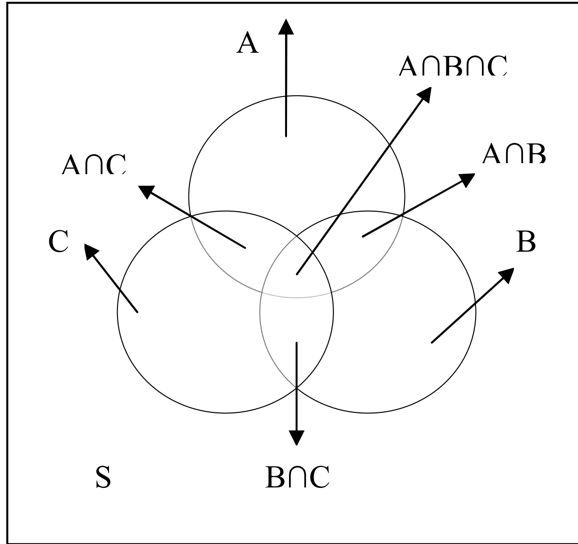
Şekil 1.23.

Birbirini engelleyen olaylarda ortak nokta yoktur yani P(AB) = 0 olmaktadır.



Şekil 1.24

Küme notasyonu kullanılırken A + B olayı **A U B** (bileşim) olarak,
AB olayı da **A∩ B** (kesişim) olarak gösterilir. Venn Diyagramı Şekil 1.25'te gösterilmiştir:



Şekil 1.25

Örnek: Bir gazete bayii toplam 200 kişinin A,B,C dergilerine abone olma sayılarını aşağıdaki gibi saptamıştır:

Dergi	Kişi sayısı
A dergisi	50
B dergisi	70
C dergisi	80
A ve B dergisi	15
A ve C dergisi	12
B ve C dergisi	20

A, B ve C dergisi	10
Hiç biri	37

bir kişinin bu dergilerden en az birine abone olma olasılığı :
P(hiç abone olmama) = 1- (37/200) = 0.815

Bir kişinin A veya C dergisine abone olma olasılığı:

P(A + C) =P(A) + P(C) – P(AC) = (50 / 200) + (80 / 200) – (12/ 200) = 0.59

Olay	Olasılık
A olayı olması için olasılık	$P(A) \in [0,1]$
A olayı olmaması için olasılık	$P(\overline{A}) = 1-P(A)$
A veya B olması için olasılık	$P(A\cup B)= P(A) + P(B) - P(A\cap B)$
A ve B olması için olasılık	$P(A\cap B) =P(A\|B)P(B)$ $=P(B\|A)P(A)$ $=P(A) P(B)$ Eğer A ve B Bağımsızlarsa
B verilmiş A olması (B koşullu A)	$P(A\|B) = P(A\cap B) /P(B)$

Tablo 1.17. : Farklı olayların olasılıkları

Bayes Teoremi

Thomas Bayes tarafından geliştirilen, koşullu olasılıkların hesaplanmasında kullanılan bir teoremdir. Bayes teoremi bir stokastik süreç sırasında ortaya çıkan bir rastgele olay A ile bir diğer rastgele olay B (eğer B için kaybolmamış olasılık varsa) için koşullu olasılıkları ve marjinal olasılıkları arasındaki ilişkidir, yani

$$P(A|B) = \frac{P(A) * P(B|A)}{P(B)}$$

Bayes teoremi formülü içinde bulunan her bir terime özel isimler verilmektedir:

- P(*A*) terimine *A* için önsel olasılık veya marjinal olasılık adı verilir. Bu önseldir, çünkü *B* olayı hakkında önceden herhangi bir bilgiyi içermemektedir.
- P (*B*|*A*) terimi verilmiş *A* için *B*'nin koşullu olasılığı adını taşır.
- P(*A*|*B*) terimi verilmiş *B* için *A*'nın koşullu olasılığı adını alır.
- P(*B*) terimi *B* olayı için 'önsel' olasılıktır veya *B*'nin marjinal olasılığıdır ve matematiksel rolü normalize eden bir sabittir.

Bu şekildeki Bayes teoremini, fazla matematiksel olmadan, sezgiye dayanarak şöyle açıklayabiliriz: Bayes teoremi eğer *B* gözlemlenmiş ise, *A* gözlemi hakkındaki inançların ne şekilde güncelleştirilebileceğini ortaya çıkartır

Bayes Teoreminin Değişik şekilleri

Bayes teoremi çok kere daha ek kavramlar eklenerek, sanki daha *süslü* olarak, ifade de edilir. Bunun için önce şu ifade kullanılır:

$\mathbf{P(B)} = P(A\cap B) + \mathbf{P(}\overline{A}\cap B) = P(B|A)P(A) + P(B|\overline{A})P(\overline{A})$

Burada $\overline{A}$ (çok kere *A olmayan* olarak ifade edilen) *A* olayının tamamlayıcısı olur. Bu Bayes teoremi formülüne konulunca Bayes teoremi için yeni alternatif bir formül elde edilir:

$$P(A|B) = \frac{P(A) * P(B|A)}{P(B|A)P(A) + P(B|\overline{A})P(\overline{A})}$$

Daha genel olarak, $\{A_i\}$ olay uzayının bir bölüntüsünü oluşturduğu göz önüne alınca, bu bölüntü içinde bulunan herhangi bir A_i için şu ifade elde edilir: B olayı önsel olarak verilmiş ise, buna göre herhangi A_i'nin olma olasılığı $P(A_i|B)$ aşağıdaki şekilde hesaplanır.

$P(B)=\sum_{i=1}^{n} P(A_i).P(B \mid A_i)$ şeklindedir. Bu durumda

$$P(A_i \mid B)=\frac{P(A_i)*P(B|A_i)}{\sum P(A_i)*P(B|A_i)} \qquad i=1,2,3,....n$$

$P(A_i)$ ile A_i olayının olasılığı,

$P(B|A_i)$ ile de A_i olayının ortaya çıkması durumunda B'nin olasılığı gösterilmektedir.

Örnek: Maria bir gün sonra evlenecek ve düğün töreni çölde yapılacaktır. Son yıllarda çölde her yıl sadece 5 gün yağmur yağmıştır. Ancak hava tahmincisi düğün günü yağmur yağacağını öngörüyor ve tahmincinin öngörüleri %90 oranında doğru çıkıyor.Yağmur yağmadığı zaman, yanlış olarak %10 ile yağmur tahmini yapıyor. Maria'nın düğün günü yağmur yağma olasılığı nedir?

Çözüm: Örnek uzayı yağar ve yağmaz olarak karşılıklı iki olay ile tanımlanır. Ek olarak üçüncü olay hava tahmincisinin yağar öngörüsüdür. Bu olaylar için gösterilim;

- Olay A_1. Maria'nın düğününde yağmur yağar.
- Olay A_2. Maria'nın düğününde yağmur yağmaz
- Olay B. Tahmincinin öngörüsü yağar.

Olasılıkların terimleriyle aşağıdakileri biliriz.:

- $P(A_1) = 5/365 = 0.0136985$ [Yılda 5 gün yağmasının olasılığı.]
- $P(A_2) = 360/365 = 0.9863014$ [360 gün yağmamasının olasılığı.]
- $P(B \mid A_1) = 0.9$ [Yağdığı durumda, tahminci nin öngörüsünün doğruluğu 90% dır.]
- $P(B \mid A_2) = 0.1$ [Yağmadığı durumda, tahminci nin öngörüsünün doğruluğu 10% dır..]

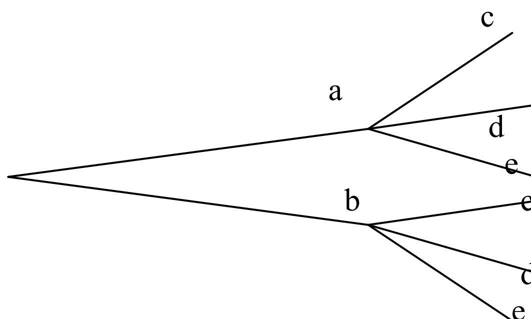
Tahmincinin yağmur yağacak öngörüsüne rağmen Maria'nın düğününde yağmur yağma olasılığını $P(A_1 \mid B)$bulmak istiyoruz. Cevap Bayes teorem ile aşağıdaki şekilde bulunabilir.

$$P(A_1 \mid B)=\frac{P(A_1)*P(B \mid A_1)}{P(B \mid A_1)P(A_1)+P(B \mid A_2)P(A_2)}$$

$P(A_1 \mid B) = (0.014)(0.9) / [(0.014)(0.9) + (0.986)(0.1)] = 0.111$ olarak bulunur.

1.10.2 Permütasyon ve Kombinasyon

Bileşik olayların olasılıklarının hesaplanmasını kolaylaştırmak için permütasyon(permutation) ve kombinasyon (combination) analizinden yararlanılır. Eğer bir olay $\mathbf{n_1}$ halde ortaya çıkabiliyorsa ve bu olaydan bağımsız diğer bir olay $\mathbf{n_2}$ halde ortaya çıkabiliyorsa her iki olay bir arada $\mathbf{n_1 * n_2}$ halde ortaya çıkabilecektir. Birinci olayın 2, ikinci olayın da 3 halde meydana çıkması durumunu ağaç diyagramı ile aşağıdaki gibi gösterebiliriz.



Birinci olayın şıkları a ve b, ikinci olayın şıkları c,d ve e ile gösterilmektedir. Her iki olay bir arada 6 defa ortaya çıkmaktadır.

a – c   b – c
a – d   b – d
a – e   b - e

Permütasyon

n birimlik kütle içinden **r** birimlik gruplar alarak bunları, değişik sırayı değişik hal sayarak yerleştirir veya sıralarsak sıralamaların herbiri bir permütasyon olacaktır. Diğer bir deyişle birimlerin sıralanışlarının önemli olduğu gruplara permütasyon adı verilir. **n** birimlik grup içinden **r** birimlik gruplar seçerek meydana getirilecek permütasyon sayısı;

$${}_nP_r = n(n-1)(n-2)\ldots\ldots\ldots\ldots(n-r+1)$$

formülü (n-r)! ile çarpıp bölersek;

$${}_nP_r = \frac{n!}{(n-r)!}$$

formülü bize çekim iadesiz yapıldığında permütasyon sayısını verir. **n** adet birimden **r** birim iadeli olarak çekiliyorsa permütasyon sayısı;

$${}_nP_r = n^r$$ formülü ile elde edilir.

Örnek: 1,2 ve 8 rakamlarından kaç adet 2 rakamlı sayı oluşturulabilir ? (çekimler iadesiz)

$${}_3P_2 = \frac{3!}{(3-2)!} = 6$$ adet, sayılar: 12,18,28,21,81,82

Bu örneği çekimlerin iadeli yapıldığını kabul ederek hesaplarsak, her rakamın tekrarlanma olanağı doğduğu için permütasyon sayısı;

$${}_3P_2 = 3^2 = 9$$ olacaktır.   sayılar: 11,12,18,22,21,28,81,82,88

Kombinasyon

Kombinasyonlarda birimlerin sıraları önemli değildir. **n** birimden oluşan bir gruptan **r** birim seçilerek gruplar oluşturuluyorsa, sıralar önemsiz ve çekim iadesiz yapılıyorsa mümkün kombinasyon sayısı;

$${}_nC_r = \frac{n!}{r!(n-r)!}$$

Örnek: 9 soru arasından 6 soru kaç şekilde çekilebilir ?

$${}_9C_6 = \frac{9!}{6!(9-6)!} = 84$$

Kombinasyon-Olasılık ilişkisi

Örnek: Bir kutuda 6 kırmızı, 4 siyah top vardır. Kutudan rastgele 3 top çekildiğinde bunların;

- Üçünün de kırmızı olma olasılığı,
- Üçünün de siyah olma olasılığı,
- En az birinin kırmızı olma olasılığı nedir ?

Birinci,ikinci ve üçüncü çekişlerde kırmızı top çekme olaylarını E1,E2 ve E3 ile gösterelim. Olayların bir arada ortaya çıkma olasılığı;

P(E1 E2 E3) = P(E1) *P(E2\E1)* P(E3\E1E2) = (6/10)*(5/9)*(4/8) = (1/6)

Kombinasyonla hesaplarsak; $\frac{6 \text{ kirmizi toptan üçünün seçimi}}{10 \text{ toptan üçünün seçimi}} = \frac{{}_6C_3}{{}_{10}C_3} = \frac{(6!/(3!*3!))}{(10!/(3!*7!))} = (20)/120 = 1/6$

Üçünün de siyah olma olasılığı olasılıkla aşağıdaki gibi hesaplanır :

(4/10)*(3 / 9) * (2 / 8) = (1 / 30)

Kombinasyonla:

$$\frac{{}_4C_3}{{}_{10}C_3} = (4/120) = 1/30$$

En az birinin kırmızı olma olasılığı ise,1'den hepsinin siyah olma olasılığı çıkarılarak bulunur

P(en az 1 Kırmızı) = 1 - (1 / 30) = (29 / 30)

1.10.3 Rastsal(Tesadüfi) Değişkenler ve Olasılık Dağılımları

matematiksel beklenen değer

Bir değişkenin beklenen değeri, o değişkenin olasılıklarına göre ağırlıklı ortalaması olarak tanımlanabilir. Süreksiz tipte dağılımların olduğu durumda **E** (expected value) matematik beklenen değeri göstermek üzere P_1, P_2,.... P_n olasılıkları ile $x_1, x_2, ..., x_n$ değerleri alabilen **x** ayrık tipte rastsal değişkeninin beklenen değeri:

$E(x) = x_1 * P_1 (x1) + x_2 * P_2(x_2) + ... + x_n * P_n(x_n)$

$E(x) = \sum x_i * P_i$

Beklenen değerin özellikleri:

- E(c*x) = c*E(x) dağılmayı gösteren her x değeri bir sabit(c) ile çarpıldığında beklenen değer de o sabit ile çarpılmış olunur.
- $E(x_1+x_2) = E(x_1) + E(x_2)$ iki ayrı dağılıma ait değerlerin toplanması ile oluşan beklenen değer, orijinal dağılımların beklenen değerleri toplamına eşittir.

Örnek: 4 madeni para birlikte atıldığında yazı gelme olayının beklenen değerini hesaplayınız.

Yazı Sayısı	Mümkün olan Sonuçlar	Olasılık($P(x_i)$)	$x_i * P(x_i)$
0	TTTT	1/16	0(1/16)
1	YTTT,TYTT,TTYT,TTTY	4/16	1(4/16)
2	YYTT,YTTY,YTYT,TYTY,TYYT,TTYY	6/16	2(6/16)
3	YYYT,YYTY,YTYY,TYYY	4/16	3(4/16)
4	YYYY	1/16	4(1/16)

$E(x) = \Sigma x_i P(x_i) = 32/16 = 2$

4 madeni para birlikte atıldığında ortalama 2 yazı gelmesi beklenmektedir.

Rastsal(tesadüfi) değişkenin varyansı ve standart sapması

Varyans $\sigma^2 = \sum (x_i - \bar{x})^2 * p(x_i)$ i=1,2,.....,k

Standart sapma: $\sigma = \sqrt{\sigma^2}$

Para atışı örneğinin varyansı standart sapması:

Aritmetik ortalama: 2

$(x_i - \bar{x})^2$	$(x_i - \bar{x})^2 * p(x_i)$
4	4*1/16
1	1*4/16
0	0*6/16

1	1*4/16
4	4*1/16

$\sigma^2 = 16 / 16 = 1$ $\sigma = \sqrt{1} = 1$

Örnek: Bir zar atıldığında beklenen değer, varyans ve standart sapma nedir?

x_i	$P(x_i)$	$x_i P(x_i)$	$(x_i - \bar{x})^2$	$(x_i - \bar{x})^2 * p(x_i)$
1	1/6	1/6	6,25	1,042
2	1/6	2/6	2,25	0,375
3	1/6	3/6	0,25	0,042
4	1/6	4/6	0,25	0,042
5	1/6	5/6	2,25	0,375
6	1/6	6/6	6,25	1,042

$\bar{x} = 21/6 = 3,5$ E(x)= $\bar{x} = x_i P(x_i)$ =21/6 =3.5

$\sigma^2 = 2.918$ Standart sapma= $\sigma = \sqrt{2,918} = 1,708$

Beklenen değer 3.5 ve herhangi bir sayının bu değerden ortalama farkı 1.708 dir.

1.10.4 Olasılık Dağılımları (Probability Distribution)

x rastsal değişkeninin tüm mümkün sonuçlarının olasılıkları hesaplandıktan sonra, karşılarına olasılıklar yazılarak iki sütun halinde olasılık dağılımları gösterilir. **x** değerleri yatay eksende, olasılıkların da dikey eksende gösterildiği grafiklerde, noktalar birleştirilerek kesikli veya kesiksiz bir eğri çizilir. Bu eğriye ***olasılık fonksiyonu***(Probability Functions) adı verilir.**x** değişkeni sürekli ise, olasılık dağılımı, ***sürekli olasılık dağılımı***(continuous probability distribution), **x** değişkeni süreksiz ise, ***süreksiz olasılık dağılımı***(discrete probability distribution) olarak adlandırılır.

Bir değer aralığında sadece tam sayılarla ifade edilebilen bazı değerleri alabilen süreksiz değişkenler, ***Binom***, ***Hipergeometrik***,***Poisson*** dağılımı göstermektedirler. Bir değer aralığında tüm değerleri alan ***sürekli*** değişkenlerin dağılımı da ***Normal*** dağılım göstermektedir.

Binom Dağılımı

Birçok deneyde iki farklı sonuç ortaya çıkmaktadır. Bir sınav sonucu başarılı ve başarısız olmak üzere iki durumda tanımlanabilir ya da kalite kontrolü için alınan bir ürün sağlam veya kusurlu olarak iki şekilde ortaya çıkabilir. Bu türde iki sonucu olan deneyler " ***Bernoulli Deneyleri veya Süreçleri***" olarak adlandırılır. Bernoulli süreci, her deneyde birbirini engelleyen iki sonuçtan birinin gerçekleştiği bir süreçtir. Madeni para atışı deneyinde her deneyde yazı(Y) ve tura(T) mümkün sonuçlarından sadece biri gerçekleşir ve her atışta P(Y) ile P(T) olasılıkları deneyler birbirinden bağımsız olduğu için aynıdır(1 / 2).

Bernoulli deneylerinde ortaya çıkan iki sonuçtan biri ***başarı*** diğeri ise ***başarısızlık*** olarak adlandırılır. p başarı olasılığını, q'da başarısızlık olasılığını göstermektedir((1- p) = q).

Deney **n** defa tekrarlanırsa toplam başarılı durum sayısı **x** ile gösterilen bir rastgele değişkendir. Bu değişken ***binom değişkeni*** adını alır.**x** değişkenini binom değişkeni olarak kabul edebilmemiz için tekrarlanan deneylerin birbirlerinin aynı olmaları, olasılıkların deneyden deneye değişmemesi, seçimlerin iadeli yapılması gerekir.

Genel olarak **n** Bernoulli deneyinde **p**=başarı olasılığı,**q**=başarısızlık olasılığı olmak üzere **k** sayıda başarı olasılığı aşağıda verilen binom olasılık fonksiyonu kullanılarak hesaplanır;

$P(k) = {}_n C_k \, p^k * q^{n-k} = (n! / (k!(n - k)!))* \quad p^k * q^{n-k}$

k'nın bütün hallerinin hesaplanması ile k'nın olasılık dağılımı elde edilir. Bu dağılıma ***Binom dağılımı*** adı verilir. Binom olasılıkları standart "Binom Dağılımı Tabloları" kullanılarak hesaplanabilir. Çeşitli p ve n değerleri için k'nın (x'in) alabileceği tüm değerlerin olasılıkları bu tablolarda verildiğinden istenilen bir x için olasılık bulunabilir.

Binom dağılımının ortalaması; $E(x) = \bar{x} = n*p$

Varyansı ve standart sapması;

$$\sigma^2 = \Sigma\ (xi - \bar{x})^2 = n*p*q \qquad \sigma = \sqrt{n*p*q}$$

Binom dağılımındaki p ve q olasılıkları birbirine eşitse dağılımın şekli simetrik olacaktır. Para atışı deneyinde p ve q olasılıkları aynı olduğu için dağılım simetrik olacaktır. p'nin q'ya eşit olmadığı durumlarda ise, dağılımın şekli asimetriktir.

Örnek: 6 defa atılan bir madeni paranın tam olarak 2 defa tura gelmesi olasılığı nedir ?

Simetrik binom dağılımı, p ve q birbirine eşit.

n = 6 , x =2, p=0.50, q= 0.50

$P(x=2) = {}_6C_2\,(0.50)^2 * (0.50)^{6-2} = (6!/(2!(6-2)!)) * (0.50)^2 * (0.50)^4 = 0.23$

Binom Dağılım tablosunu kullanarak hesaplarsak;

P(x;n,p)= P(2;6, 0.50) = (0.3438 – 0.1094) = 0.2344

Aynı 6 atışta en az 4 defa tura gelmesi olasılığı ise tablodan şu şekilde hesaplanabilir;

$P(x \geq 4) \longrightarrow P(3; 6, 0.50) = 0.6562$

$P(x \geq 4) = 1 - 0.6562 = 0.3438$

Veya

P(x=0)+P(x=1)+P(x=2) = 0.3438

Ortalama durum hesaplama karmaşıklığı

Bir algoritmanın ortalama durum hesaplama karmaşıklığı bir rastgele değişkenin beklenen değeri olarak yorumlanabilir. Bir deneyin örnek uzayı olası girişler a_j, j=1,2,,….,,n olarak ve X, verilen a_j girişini kullanan algoritmanın işlem sayısını a_j' ye atayan rastgele değişken olsun. Her bir olası a_j'girişi için olasılık $p(a_j)$ olarak verilsin. Bu durumda algoritmanın ortalama durum karmaşıklığı

$E(X) = \sum_{j=1}^{n} p(a_j)X(a_j)$ dir. Bu X 'in beklenen değeridir.

Örnek: Doğrusal arama algoritmasının ortalama durum karmaşıklığının hesabı: n elemanlı listede bir x elemanının aranmasını x'in listede olma olasılığını p kabul ederek hesaplayalım.

Çözüm: Eğer x, listede i. Eleman ise x'i bulmak için 2i+1 karşılaştırma yapılacaktır. Eğer x listede yok ise 2n +2 karşılaştırma yapılacaktır. a_i'ye eşit olan x'in n elemanlı listede olma olasılığı p/n ve listede olmama olasılığı ise q=1-p dir. Bu durumda doğrusal arama algoritmasının ortalama durum karmaşıklığı; E=3p/n + 5p/n+……+(2n+1)p/n +(2n+2)q olacaktır.

$=p/n(3+5+\ldots+(2n+1)) + (2n+2)q = p((n+1)^2-1)/n + (2n+2)q = p(n+2)+(2n+2)q$ dir.

Bu sonuçta eğer x listede mutlaka var ise p=1, q=0 olacak E= n+2 bulunacak. Eğer x'in listede bulunma olasılığı ½ ise q=1-p =1/2 olacak E = (n+2)/2 +n+1= (3n+4)/2 olacaktır.Eğer x listede mutlaka yok ise p=0, q=1 olacak ve E= 2n+2 bulunacaktır.

1.11 Asimtotik Notasyonlar

Matematikte, büyük O notasyonu(Sembol O olduğu için bu şekilde adlandırılır), genellikle daha basit fonksiyonlar olan, çok küçük ve çok büyük argümanlar için bir fonksiyonun sınırlayıcı davranışını açıklar. Aynı zamanda Büyük Oh notasyonu, Landau Notasyonu ve Asimtotik notasyon olarak adlandırılır. İlgili sınırlar için, *o*, Ω, ω, ve *Θ* gibi diğer semboller vardır.

Her ne kadar, bu notasyonlar, bir algoritmanın hesaplama kaynaklarını, girişin büyüklüğünü nasıl etkilediğini(genellikle çalışma zamanı ve bellek) açıklamak için karmaşıklık kuramında, matematiğin bir parçası olarak geliştirilmiş olsa da, bu notasyonlar benzer kestirimleri yapmak için çoğu bilimsel ve matematiksel alanda kullanılır.

Şimdi iki algoritma karmaşıklığını nasıl karşılaştıracağımızı düşünelim. f(n), giriş boyutu n'in bir fonksiyonu olarak ifade edilen algoritma'nın en kötü durumdaki maliyet fonksiyonu, ve g(n) diğer algoritmanın maliyet fonksiyonu olsun. Örneğin, sıralama algoritmaları için, 10 elemanlık bir listeyi alan f (10) ve g (10) algoritmalarının maksimum sayıda adımları olacaktır. Eğer, tüm $n\geq 0$ için, f(n), g(n)'e eşit veya daha küçük ise, buradan karmaşıklık fonksiyonu f olan algoritma kesinlikle daha hızlıdır. Ancak, genel olarak, hesaplama maliyeti ile olan ilgimiz büyük girişleri olan durumlar içindir; böylece n küçük değerleri için f(n) ve g(n)'in karşılaştırılması, f(n) ve g(n)'in bir eşik değerinden büyük n için karışaştırılması daha az anlamlıdır.

Burada algoritmaların tam hızlarından çok, performans sınırları hakkında yorum yapmaktayız. Kart kümesini sıralamak için gerekli olan adımların gerçek sayısı elimizdeki kartların başlangıçtaki sayısına bağlıdır. Adımların her birini gerçekleştirmek için gerekli zaman işlemci hızı, işlemci önbellek durumu, vb..'na bağlıdır. Somut ayrıntılar çok karmaşık olup, sıralama algoritmasının özü ilgili değildir.

1.11.1 Tanımlar

Büyük O notasyonu ,(f(n)'in egemen terimi **olsa olsa** olan fonksiyonları içerir**)** Pratikte, büyük O notasyonu, bir algoritmanın gücünün(bu güç f(n) fonksiyonu olarak gösterilir) büyümesindeki sıkı üst sınırı(upper bound) göstermek için kullanılır Küçük o notasyonu o() ise sıkı olmayan üst sınırı açıklamak için kullanılır.

Büyük O: O(g(n)) : f(n) ve g(n) pozitif tamsayıları pozitif gerçel sayılara dönüştüren fonksiyonlar olsunlar.

Eğer, $\forall n \geq n_0$ için $|f(n)| \leq c\ |g(n)|$ koşulunu sağlayan öyle bir sabit $c > 0$ ve $n_0 \geq 1$ varsa, f(n) fonksiyonu = O(g(n)) dir. (veya $f(n) \in O(g(n))$) (g(n) in büyük O notasyonu).

Küçük o : o(f(n)) (f(n)'in egemen terimi **'den tam olarak küçük** olan fonksiyonları içerir**)**

f(n) ve g(n) pozitif tamsayıları pozitif gerçel sayılara dönüştüren fonksiyonlar olsunlar.

Eğer, $\forall n \geq n_0$ için $|f(n)| < c\ |g(n)|$ koşulunu sağlayan öyle bir sabit $c > 0$ ve $n_0 \geq 1$ varsa, f(n) fonksiyonu = o(g(n)) dir. (veya $f(n) \in o(g(n))$) (g(n) in küçük o notasyonu).

Diğer taraftan, O(n) ve o(n) 'e paralel olarak f(n)'in sıkı ve gevşek alt sınırlarını tanımlamak mümkündür. Büyük Omega(**Ω** ()) sıkı alt sınırı ve küçük omega(ω ()) gevşek alt sınırı tanımlar.

Büyük Omega: Ω(f(n)) (f(n)'in egemen terimi **en azından** olan fonksiyonları içerir**)** Algoritmalarda sıkı alt sınırı(lower bound) açıklamak için kullanılır.

f(n) ve g(n) pozitif tamsayıları pozitif gerçel sayılara dönüştüren fonksiyonlar olsunlar.

Eğer, $\forall n \geq n_0$ için $|f(n)| \geq c\ |g(n)|$ koşulunu sağlayan öyle bir sabit $c > 0$ ve $n_0 \geq 1$ varsa,

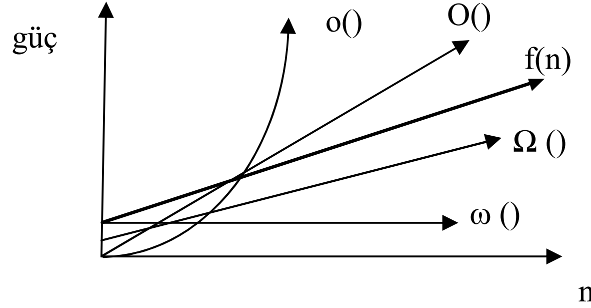
f(n) fonksiyonu = Ω (g(n)) dir. (veya f(n) $\in \Omega$ (g(n))) (g(n) in büyük Ω notasyonu).

Küçük omega: ω(f(n))

f(n) ve g(n) pozitif tamsayıları pozitif gerçel sayılara dönüştüren fonksiyonlar olsunlar.

Eğer, $\forall n \geq n_0$ için $|f(n)| > c\ |g(n)|$ koşulunu sağlayan öyle bir sabit c >0 ve $n_0 \geq 1$ varsa, f(n) fonksiyonu = **ω** (g(n)) dir. (veya f(n) $\in$ **ω** (g(n))) (g(n) in küçük **ω** notasyonu).

Bu notasyonlar arasındaki bağıntı Şekil 1.26'de gösterilmiştir.



Şekil 1.26

Tanımlanan dört terim arasındaki anahtar özellikleri tablo 1.17 'da gösterilmiştir.

Tablo 1.17

Tanım	c>0	no≥1	f(n) c.g(n)	Anlam
O()	∃	∃	≤	En fazla, üst sınır
o()	∀	∃	<	nadiren
Ω()	∃	∃	≥	En azından, alt sınır
ω()	∀	∃	>	

Ω() ve ω(), algoritmaları açıklamakta çok sık olarak kullanılmazken, yeni bir tanım yapmak için O() ve Ω() 'yı kullanabiliriz. Yeni Tanım büyük Teta Θ() dır. Bir algoritmanın Θ(n)'i denildiğinde, algoritmanın gücünün artışında sıkı üst sınırı ve sıkı alt sınırı birlikte ifade edilir.

Büyük Teta: Θ(f(n)) (f(n)'in egemen terimi **'a eşit** olan fonksiyonları içerir**)**

f(n) ve g(n) pozitif tamsayıları pozitif gerçel sayılara dönüştüren fonksiyonlar olsunlar.

Eğer, Ancak ve ancak , f(n) $\in$ O(g(n)) ve f(n) $\in \Omega$ (g(n)) ise, f(n) fonksiyonu = **Θ** (g(n)) dir. (veya f(n) $\in$ **Θ** (g(n))) (g(n) in büyük **Θ** notasyonu).

Uygulama Örnekleri

1. f(n) = 7n+8 ve g(n) = n verilsin. f(n) $\in$ O(g(n)) midir?

Çözüm: 7n+8 $\in$ O(n) olması için, c ve n_0'ı $7n+8 \leq c.n$, $\forall n \geq n_0$ inceleme ile, c'nin 7'den büyük olması gerektiği açıktır.

Şimdi, uygun bir n_0 bulunmalıdır. Bu durumda, f(8)=8.g(8) dir. Çünkü, O() 'nın tanımı, $f(n) \leq c$ .g(n) olmasını gerektirir. Eğer n_0= 8 ve 8'den büyük herhangi bir tamsayı seçilirse bütün n_0 lar için çalışır.

Buradan, $7n+8 \leq c\ .n$ 'i $\forall n \geq n_0$'lar için sağlayacak, c ve n_0 sabitleri bulunmuş oldu, böylece, 7n+8 $\in$ O(n) denilebilir.

2. f(n) = 7n+8 ve g(n) = n verilsin. f(n) $\in$ o(g(n)) midir?

Herhangi bir c için bunun doğru olması için, f(n) < c g(n) 'i asimtotik olarak doğru yapan bir

n_0 bulabilmemiz gerekir. Bununla birlikte, bu doğru gözükmez. 7n +8 ve n doğrusaldır ve o() gevşek üst sınırı tanımlar. Bunun doğru olmadığını göstermek için, bir sayıcı örneğine ihtiyaç vardır.

Çünkü iddianın doğru olması için herhangi bir c>0 çalışmalıdır, çalışmayacak bir c bulalım. c=100 verilsin. 7n+8 < 100n olan bir n_0 bulabilirmiyiz? Bulunabilir örn. n_0=10. Şimdi c=1/100 olsun. 7n+8 < n.1/100 olan bir n_0 bulabilirmiyiz? Elbette bulunamaz. Bu nedenle $7n+8 \notin o(n)$ dir. Bunun anlamı; g(n)=n 7n+8 üzerinde bir gevşek üst sınır değildir.

3. $7n+8 \in o(n^2)$ midir?

Tekrar, bunu iddia etmek için herhangi bir c için $7n+8 < c\cdot n^2$ yapan bir n_0 bulmalıyız. Örnekleri hatırlayarak, herhangi bir c için bir n_0 bulunabileceğini göstermek gerekir.

Eğer c=100 ise eşitsizlik açık olarak doğrudur. Eğer c=1/100 ise, bir miktar hayal gücü kullanmak gerekir fakat bir n_0 bulunabilir(n_0=1000 dene)

Bu noktada, seçilen c ne olursa olsun, sonuçta $c.n^2$ yi 7n+8'e hakim kılabilmeliyiz.(Bunun anlamı, tanımı doğrulamak için yeterli büyüklükte bir n_0 bulunabilir) Sonuçta, $7n+8 \in o(n^2)$ dir.

1.12 Toplamlar

Diziler ve Toplamlar(Sequences and Summations)
Bir dizi, doğal sayılar alanında bir fonksiyondur. Diziler için f(x) notasyonu yerine a_n kullanılır. Tüm pozitif sayılar alanının kullanan sonsuz diziler olduğu gibi ilk n pozitif sayılar alanının kullanan sonlu diziler de olabilir.
Bir diziyi tanımlamak için genel terim(n. terim veya a_n) yazılmalıdır. ;Bazen ilk birkaç terimi verilen birden fazla dizi olabilir.

Dizi tanımı

Bir dizi genel terimi belirtilerek iki farklı şekilde tanımlanabilir.
Genel Terim, a_n
Öncelikle, terimlerin sayısının n, bağlı olduğu bir biçim kullanılmalıdır. Genel terim biliniyorsa ilk beş terimi bulmak için, genel terimdeki n'i 1,2,3,4 ve 5 ile değiştirmek ve basitleştirmek gerekir..
Genel terimi a_n = 3n-2 olan diziyi düşünelim.İlk beş terim n yerine 1,2,3,4 ve 5 koyarak bulunur.
a_1= 3(1) - 2 = 1
a_2= 3(2) - 2 = 4
a_3= 3(3) - 2 = 7
a_4= 3(4) - 2 = 10
a_5= 3(5) - 2 = 13
Buradan dizinin ilk beş terimi 1, 4, 7, 10, 13 olarak bulunur.
Bir başka örnek olarak genel terimi a_n = 1 / n. olarak tanımlanan diziyi düşünelim.
Dizinin ilk beş terimi 1/1, 1/2, 1/3, 1/4, ve 1/5. olarak bulunur.
Yinelemeli(Recursive) Tanım
Bir diziyi tanımlamak için ikinci yol yinelemeli tanımlama şeklidir. Yinelemeli tanım, bir dizide sonraki terimi tanımlamak için mevcut ve/veya önceki terimi kullanır. Sonraki terim olarak a_{k+1} mevcut terim a_k ve önceki terim ise a_{k-1} olarak düşünülür.

Örnek: a_1 = 5 ve a_{k+1} = 2 a_k - 1.olduğu diziyi düşünelim."Bu ifade, sonraki terim mevcut terimin iki katının bir eksiği" olarak okunabilir.

İlk beş terim:
a_1= 5 Tanımdan
a_2= 2(5) - 1 = 9

a_3= 3(9) - 1 = 17
a_4= 3(17) - 1 = 33
a_5= 3(33) - 1 = 97

Örnek: a_1 = 2, a_2 = 1, ve a_{k+2} = 3a_k - a_{k+1}olarak tanımlanana diziyi düşünelim. Bunu iki sonraki terim mevcut terimin üç katından bir sonraki terim çıkartılarak bulunur.
İlk beş terim den ilk ikisi tanımdan sonrakiler ise ifadeden bulunur.

Fibonacci Dizileri
Dizilerin yinelemeli tanımına en meşhur örnek, Fibonacci dizileridir. İlk iki terim 1 olarak tanımlanır. Sonraki terimler kendinden önce gelen iki terimin toplamı olarak tanımlanır.
1, 1, 2, 3, 5, 8, 13, 21,…
Fibonacci dizisi 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, ... $a_{n+1} = a_n + a_{n-1}$. şeklindedir.
Fibonacci dizilerine tabiatta sık sık rastlanır. Örneğin birçok bitkinin (kiraz, karaağaç, armut) gövdesindeki yapraklar. Seçilen bir daldaki yaprakları dala doğrudan erişene kadar sayılırsa genellikle Fibonacci sayısı şeklindedir. Bir çam kozalağındaki sağ ve sol spiraller, ayçekirdeği başı, veya ananaslar sayılırsa iki sayı sıklıkla Fibonacci sayılarıdır.

Faktöriyeller !

Faktöriyel sembolü olarak **!** kullanılır. Bir pozitif tamsayının faktöriyeli, o sayıya eşit ve küçük olan tüm pozitif tamsayıların çarpımıdır. Sıfır faktöriyel özel bir durumdur ve 0! = 1 dir.
Tanımdan yola çıkarak;.
1! = 1
2! = 2*1! = 2*1 = 2
3! = 3*2! = 3*2*1 = 6
4! = 4*3! = 4*3*2*1 = 24
5! = 5*4! = 5*4*3*2*1 = 120
n! = n(n-1)! = n*(n-1)*(n-2)*...3*2*1 yazılabilir.
Burada faktöriyelin yinelemeli tanımı söz konusudur ve "Herhangi bir sayının faktöriyeli, kendinden bir küçük sayının faktöriyeli ile kendisinin çarpımına eşittir" şeklinde tanımlanır.
Sigma /Toplam Notasyonu
Toplam, matematikte çok sık kullanılan ve Yunan harfi büyük sigma toplam sembolü ile gösterilen bir kavramdır. Bu notasyon dizilerin terimlerinin toplamını göstermekte ve hesaplamakta kullanılır. Örneğin $\{a_1,a_2,a_3,\ldots\ldots\ldots a_n\}$ şekilde terimleri olan dizinini terimleri toplamı;

$\sum_{k=1}^{n} a_k = a_1 + a_2 + a_3 + \ldots\ldots\ldots + a_n$ şeklinde gösterilir. Burada k toplamın göstergesi, k=1 toplamın alt sınırı, k=n ise üst sınırıdır.
Örnekler:

$$\sum_{k=1}^{5}(3k-2)$$

3k-2 ifadesinde k'nın değerlerinin 1 ila 5 arasında değiştirip sonuçları toplarsak,
[3(1)-2] + [3(2)-2] + [3(3)-2] + [3(4)-2] + [3(5)-2] = 1 + 4 + 7 + 10 + 13 = 35 elde edilir.

$\sum_{k=1}^{5} 3k - 2$ ifadesini ele alırsak;

[3(1) + 3(2) + 3(3) + 3(4) + 3(5)] - 2 = [3 + 6 + 9 + 12 + 15] - 2 = 45 - 2 = 43 bulunur.
Her ne kadar ifadeler benzer olsalar da sonuçlar farklıdır. İkinci örnekte çarpma işleminin çıkarmaya göre önceliği olduğundan toplam sadece ilk terim için uygulanmıştır.

Toplamın Özellikleri

Toplamın aşağıdaki özellikleri göstergenin alt ve üst limitleri belirtilmeden verilmiştir. Basitlik için k=1 ve n yazılmamıştır.

Toplamın sonucu bir sabit ile çarpılabilir.

$\sum ca_k = c\sum a_k$

Burada a_k 'nın bir alt göstergesi varken c'nin olmadığına dikkat edilmelidir. Bunun anlamı, c bir sabit ve a, k'nın fonksiyonudur. Sabitle çarpılan bir fonksiyonun toplamı, fonksiyonun toplamının sabitle çarpımıdır.

Bir toplamın toplamı, toplamların toplamıdır.

Bunun anlamı, toplam sembolünün toplama altında dağılabileceğidir..

$\sum (a_k + b_k) = \sum a_k + \sum b_k$

Farkın toplamı, toplamların farkına eşittir.

Bunun anlamı, toplam sembolünün çıkarma altında dağılabileceğidir.

$\sum (a_k - b_k) = \sum a_k - \sum b_k$

Tablo 1.18. Örnek Toplamlar ve genel ifadeleri

Toplam	Genel Formu
$\sum_{k=0}^{n} ar^k$	$\frac{ar^{n+1} - a}{r-1}$, r≠1
$\sum_{k=0}^{n} k$	$\frac{n(n+1)}{2}$
$\sum_{k=0}^{n} (2k+1)$	$(n+1)^2$
$\sum_{k=0}^{n} k^2$	$\frac{n(n+1)(2n+1)}{6}$
$\sum_{k=0}^{n} k3$	$\frac{n^2(n+1)^2}{4}$

Örnek: $\sum_{k=50}^{100} k^2$ toplamını hesaplayalım.

Çözüm: öncelikle $\sum_{k=1}^{100} k^2 = \sum_{k=1}^{49} k^2 + \sum_{k=50}^{100} k^2$ buradan;

$\sum_{k=50}^{100} k^2 = \sum_{k=1}^{100} k^2 - \sum_{k=1}^{49} k^2$

$\sum_{k=50}^{100} k^2 = \frac{100.101.201}{6} - \frac{49.50.99}{6}$ =338.350-40,425=297,925

Problemler

A ve B' nin ortak elemanı yoksa ve C={x: x∈A∧x∈B} ise C' nin boş küme olduğunu kanıtlayınız.

1- {x: $2x^2$+5x-3=0}⊆{x: $2x^2$+7x+2=3/x} olduğunu ispatlayınız.

2- Aşağıdaki ifadelerin doğruluğunu göstermek için Venn şemalarını çiziniz.

(i) $(\overline{A - B})$=B∪$\overline{A}$

(ii) (A-B)∪ (B-A)=(A∪B)-(A∩B)

3- [0,1]={x∈IR:0≤x≤1} (0,1)={ x∈IR:0<x<1}

[0,1)= {x∈IR:0≤x<1} (0,1]= {x∈IR:0<x≤1}

olsun. Bu durumda aşağıdaki kümeleri geometrik olarak tanımlayınız.

(i) [0,1] x [0,1)

(ii) [0,1) x (0,1]

4- X x Y = X x Z ise Y=Z olmak zorunda mıdır? Açıklayınız.

5- Aşağıdaki mantıksal eşdeğerlilikleri sağlayınız.

(i) $(p \leftrightarrow q) \equiv (\overline{p \wedge \overline{q}}) \wedge (\overline{q \wedge \overline{p}})$

(ii) $(p \veebar q) \equiv \overline{\overline{(p \wedge \overline{q})} \wedge \overline{(q \wedge \overline{p})}}$

6- Aşağıdaki argümanların doğruluğunu test ediniz.

(i) Okulu bırakırsam bankada işe başlayacağım. Okulu bırakmıyorum o halde bankada işe başlamayacağım.

(ii) James polis veya futbolcudur. Eğer polisse tabancası vardır. James'in tabancası yoktur o halde James futbolcudur.

7- $n>0$ olmak üzere n^3+2n 'in 3 ile bölünebildiğini tümevarım ile ispatlayınız.

8- Herhangi üç ardışık tamsayının çarpımının 6 ile bölünebildiğini ispatlayınız.

9- İlk n pozitif tamsayının karelerinin toplamının $\frac{n(n+1)(2n+1)}{6}$ olduğunu ispatlayınız.

10- $A=Z^+ \times Z^+$ ve R, A üzerinde '(a,b)***R***(c,d) sadece ve sadece a+d=b+c ise' şeklinde tanımlanan bir bağıntı olsun. ***R*** bağıntısının yansıyan, simetrik ve geçişli olduğunu fakat ters simetrik olmadığını gösteriniz.

11- ***R***, A' dan B 'ye ve ***S***, B' den C 'ye birer bağıntı olsun. ***R*** ve ***S*** 'nin bileşkesi A' dan C 'ye $S \circ R$ bağıntısıdır ve 'a($S \circ R$)c sadece ve sadece a***R***b ve b***S***c olacak şekilde bir $b \in B$ elemanı var ise' şeklinde tanımlanmıştır.

Bu tanıma göre, ***R***, Z^+ üzerinde tanımlı bir bağıntı olsun.

n ***R*** m sadece ve sadece $m=n^2$ olduğuna göre; Z^+ üzerinde $R^2=R \circ R$ bağıntısını tanımlayınız.

A={1,2,3,4} olsun.

a. A üzerinde kaç tane eşdeğerlik bağıntısı vardır?

b. A üzerinde $(1,2) \in R$ özelliğine sahip kaç tane ***R*** eşdeğerlik bağıntısı vardır?

12- Bir R bağıntısı R^2 üzerinde şu şekilde tanımlanmıştır.

$(x_1,y_1)R(x_2,y_2)$ sadece ve sadece $x_1<x_2$ veya hem $x_1=x_2$ hem de $y_1 \le y_2$ ise.

R 'nin R^2 üzerinde bir parçalı sıra olduğunu gösteriniz.

Aşağıdaki fonksiyonların görüntülerini bulunuz.

c. f: R $\rightarrow$ R, $x \mapsto (x+2)^2$

d. f: R $\rightarrow$ R, $x \mapsto \frac{1}{(x^2+2)}$

e. f: R $\rightarrow$ R, $x \mapsto x^4$

13- . $g \circ f$ bileşke fonksiyonunu tanımlayınız

f:R $\rightarrow$ R, $f(x)=\begin{cases} x^2+x, x \ge 0 \\ 1/x \;, \quad x<0 \end{cases}$

g:R $\rightarrow$ R, $g(x)=\begin{cases} \sqrt{x+1}, x \ge 0 \\ 1/x \;, \quad x<0 \end{cases}$

14- f: A $\rightarrow$ B ve g: B $\rightarrow$ C iki fonksiyon olmak üzere,

'Hem ***f*** hem de ***g*** surjective ise $g \circ f$ bileşkesi de surjective'dir' şeklindeki teoremi ispatlayınız.

15- .f(x)=$\sqrt{2x-3}$ fonksiyonunun tersini (g(x)) bulup $g \circ f$ ve $f \circ g$ bileşke fonksiyonlarını yazarak sonucun x olduğunu ispatlayınız.

16- .f ve g $R \rightarrow R$ ve $k \in R$ olmak üzere birer fonksiyon olsun. f+g, f*g ve kf: $R \rightarrow R$ fonksiyonları sırasıyla şu şekilde tanımlanmaktadır:

(***f***+***g***)(x)=***f***(x)+***g***(x)

(***f****g***)(x)= ***f***(x)****g***(x)

(k***f***)(x)= k.***f***(x).

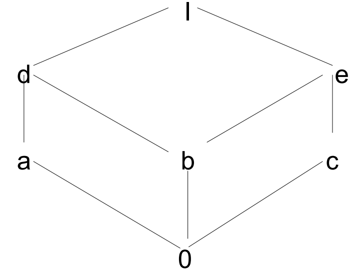
(i) Eğer $k \neq 0$ ise kf ‘in sadece ve sadece f bijeksiyon ise bijeksiyon olduğunu ispatlayınız.

(ii) Ne ***f***+***g*** ’nin ne de ***f****g*** ‘nin bijeksiyon olmadığı ***f*** ve ***g*** bijeksiyonları tanımlayınız.

17- Şekil 1.27‘deki kafeste ;

i :beş elemanlı bütün alt kafesleri bulun

ii: bu kafes dağılma özelliği gösterirmi(distributive)?



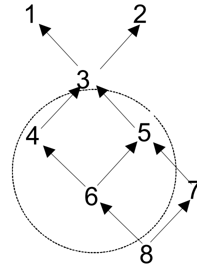
Şekil 1.27

18- B={1,2,........,7,8} şekil 1.28‘de gösterildiği gibi sıralıdır. B’nin alt kümesi olan C={4,5,6} yi ele alalım.

a. C’nin üst sınır kümesini bul

b.C’nin alt sınır kümesini bul

c. sup(C) ve inf(C) varmıdır ?



Şekil 1.28

19- .Sonlu uzunluklu sonsuz kafes için bir örnek verin.

20- . F(x,y,z) = xy +xz+yz fonksiyonunun değerinin ancak ve ancak x,y, ve z değişkenlerinin en az iki tanesinin değerinin 1 olması durumunda 1 olacağını gösterin.

21- . F(x,y,z) = $(\bar{x}+y)(\bar{x}+\bar{z})$ fonksiyonunu toplamlar çarpımı şeklinde ifade ediniz.

22- . F(x,y) = (x+y) ve G(x,y)= $\bar{x}$y+x fonksiyonlarının aynı olduğunu gösteriniz.

23- . $F(x,y,z,t)=xyzt + xy\bar{z}t + \bar{x}y\bar{z}t + \bar{x}y\bar{z}\bar{t} + \bar{x}\bar{y}\bar{z}\bar{t} + \bar{x}\bar{y}\bar{z}t + x\bar{y}\bar{z}t + x\bar{y}z\bar{t}$ ifadesini Karnaugh haritası yöntemi ile minimize ediniz.

2 Kombinatorik Teori

2.1 Kombinatorik ve temel sayma kuralları

Tanım: Matematiğin "sayma" temeline dayanan dalı. Kombinatorik nesnelerin düzeninin incelenmesidir. Kombinatoriğin en önemli alanı, belirli özelliğe sahip nesnelerin sayılmasıdır. (misal: n elemanlı bir kümeden m elemanlı bir başka kümeye yazılabilecek örten fonksiyonların adedi)

Uygulamalar:

Algoritmaların çalışma zamanlarının analizi(Karmaşıklık)

Şans Oyunları

İsteği karşılamak için yeterli IP adresi var mı?

7 karakterli kaç adet şifre olabilir?

Örnek: 3 harfi takip eden 3 rakam bulunan altı karakterli kaç adet ruhsat plakası olabilir?

Çözüm: 29.29.29.10.10.10 = 24.389.000 adet.

Çarpma Kuralı:

Temel çarpma kuralı, iki alt işten meydana gelen bir yordamı yapmak için yolların sayısı, ilk işi yapmak için gereken yol sayısı ile birinci bittikten sonra ikinci işi yapmak gereken yol sayısının çarpımıdır.

E_1, E_2,……,E_r olmak üzere r adet olay olduğu varsayılsın. Her bir E_i(i=1,n) nin olabilmesi için n_i yol var ise, önceki olay olduktan sonraki olay öncekine bağımlı değil ise, dizideki olayların olabilmesi için toplam $(n_1)(n_2)$……..(n_r) adet alternatif yol vardır.

Örn. m elemanlı A kümesinden n elemanlı B kümesine kaç adet birebir fonksiyon vardır?

Eğer m> n ise hiç fonksiyon yoktur.

Diğer durumda; A ‘daki ilk elemanı düşünelim: B'deki n adet elemana olası dönüşüm vardır. Şimdi ikinci elemanı düşünelim: B'de dönüştürülebilecek kalan n-1 eleman vardır. Devam edilirse;

n.(n-1).(n-2)……(n-m+1) adet bulunur. Eğer n=m ise, n! Kadar A'dan B'ye birebir fonksiyon vardır.

Toplama Kuralı:

Temel toplama kuralı, iki alt işten meydana gelen bir yordamı yapmak için yolların sayısı, eğer işler eşzamanlı olmuyor ise, her bir işi yapmak için gerekli yolların toplamıdır.

E_1, E_2,……,E_r olmak üzere r adet olay olduğu varsayılsın. Her bir E_i(i=1,n) nin olabilmesi için n_i yol var ise, eğer olaylar eş zamanlı olarak olmuyor ise, dizideki olayların olabilmesi için toplam $(n_1+n_2+$……..$+n_r)$ adet alternatif yol vardır.

Örnek: Bir turist grubunda, 8 Avusturyalı, 5 Brezilyalı ve 6 Kanadalı turist vardır.

Çarpma kuralı gereği;

Avusturyalı ve Brezilyalı çift sayısı 8x5=40 farklı şekilde seçilebilir.

Avusturyalı ve Kanadalı çift sayısı 8x6=48 farklı şekilde seçilebilir.

Kanadalı ve Brezilyalı çift sayısı 6x5=30 farklı şekilde seçilebilir.

Toplama kuralı gereği: gruptan farklı milletten çift seçme sayısı 40+48+30= 118 dir.

Farklı milletten 3 turist seçme alternatifi 8x5x6 olurken, tipik bir temsilci 8+5+6 farklı şekilde seçilebilir.

2.2 Permutasyonlar

n farklı nesnenin X derlemesini düşünelim. X'in r permutasyonu, X'ten alınan r adet elemanın bir satırda düzenlemesidir. Elbette r en fazla n dir. n farklı nesnenin r permutasyonu P(n,r) ile gösterilir. Herhangi r permutasyon, r olayın öncekilere bağımlı olmaksızın oluşma sayısıdır. Bu nedenle, X'ten herhangi keyfi bir nesne n farklı şekilde seçilebilir ve ikinci keyfi nesne (n-1) şekilde seçilebileceği ve devam edilip tüm r nesne seçileceği için, çarpma kuralı gereği, P(n,r)= n(n-1)(n-2)……….(n-r+1) olarak verilebilir. n=r ise P(n,r)= n! dir.

Tahsis problemi ve Permutasyonlar.

Tanımlı sırada düzenlenmiş n farklı yer ve her bir yere birden fazla eleman koyulamayacak şekilde r farklı nesneyi bu yerlere yerleştirecek şekilde düzenleyelim. Böyle bir düzenlemenin toplam sayısı, çarpma kuralı gereği P(n,r) permutasyonu ile hesaplanır.

n elemanlı X kümesinin n permutasyonu X'in Permutasyonu olarak adlandırılır ve P(n,n) =n.(n-1)(n-2)…….3.2.1 olarak n! (faktöriyel) notasyonu ile gösterilir. Genel şekli,

p(n,r) = n!/(n-r)! ile hesaplanır. (0!=1) dir

Örnek: Eğer X={1,2,3,4,5,6,7} ve r=3 ise; X'in 3'lü permutasyonu P(7,3)= 7!/(7-3)!= 5.6.7= 210 'dur.

Dairesel ve Halka Permutasyon.

Eğer nesneler dairesel olarak tekrarlayan bir diziliş şeklinde düzenlenirse, Bu durumda permutasyon n elemanlı dizi için, (n-1)! , eğer bir halka şeklinde olursa (n-1)!/2 dir.

Örnek; Mavi(M), Yeşil(Y), Kırmızı(K), Pembe(P), ve Beyaz(B) renkli taşların dizilişlerini ele alırsak,

a. Bu taşların yatay olarak farklı dizilme sayısı 5! ile hesaplanır.

b. Eğer dairesel olarak dizilişlerini ele alırsak, Bir renk sabit bırakılıp diğerleri dizilirse 4! Kadar farklı diziliş olur.(MYKPB ve MKYBP farklı) ,(MYKPB ve YKPBM aynı

c. Bu taşlar bir halka şeklinde dizilirse, her diziliş iki kere tekrar etmiş olur ve bu durumda, 4!/2 adet diziliş elde edilir.(MYKPB ve MBPKY aynı)

Genelleştirilmiş Permutasyon

Eğer n nesnenin düzeni olan X, k farklı boş olmayan ve her biri n_i adet benzer elemanlı i (i=1,2,….,k) adet grup içeriyorsa X'in genelleştirilmiş permutasyonu

$P(n;n_1,n_2,..,n_k)= (n!)/(n_1!)(n_2!).....(n_k!)$ dir.

Örnek: 9 harfin bulunduğu CONSENSUS kelimesi 6 gruba bölünür. Bir grupta 3 S, ikincide 2 N diğerleri ise birer adet farklı harf bulundurur. Bununla elde edilecek farklı dizilişler genelleştirilmiş permutasyon ile,

(9!)/(3!)(2!)(1!)(1!)(1!)(1!) =30.240 adet bulunur.

Eğer, $r \leq k$ olmak üzere, n_i (i=1,2,….,k) toplamı r olan k adet tamsayı ise $(n_1+n_2+\ldots+n_k=r)$;

$P(n;n_1,n_2,..,n_k)= P(n,r)/(n_1!)(n_2!).....(n_k!)$ dir. Burada aşağıdaki özellikler geçerlidir.

1) $P(n;n_1,n_2,..,n_{k-1})= P(n;n_1,n_2,..,n_{k-1},m)$ m==n-($n_1+n_2+..+n_{k-1}$)

2) P(n;r)= P(n;n-r) = P(n;r,n-r)

3) (r!)P(n;r)= P(n,r)

2.3 Kombinasyonlar

n farklı nesnenin koleksiyonu X olarak verilsin. X'ten r farklı nesnenin herhangi bir koleksiyonu X'in r kombinasyonu olarak adlandırılır. Diğer bir deyimle, Eğer X bir küme ise, X'in r elemanlı herhangi bir alt kümesi, X'in bir r-kombinasyonudur. r-kombinasyonda, r-permutasyonun tersine seçilen r elemanın sırası önemli değildir. n elemanlı bir kümenin r-kombinasyonu C(n,r) ile gösterilir. Burada, r alt kümenin kardinalitesidir. n elemanlı kümede P(n,2) iki elemanın sıralı çiftlerinin sayısı, C(n,2) ise sırasız çiftlerinin sayısıdır. Doğal olarak C(n,0)=C(n,n)=1 dir.

C(n,r) ve P(n,r) arasında aşağıdaki bağıntı vardır.

C(n,r) .(r!) = P(n,r)

$C(n,r) = \frac{(n!)}{r!(n-r)!}$ şeklinde ifade edilir.

Tahsis problemi ve Kombinasyonlar.

Kombinasyonları, tahsis problemine çözüm olarak farklı açıdan yorumlamak mümkündür. Tanımlı sırada düzenlenmiş n farklı yer ve her bir yere birden fazla eleman koyulamayacak şekilde r **aynı** nesneyi bu yerlere yerleştirecek şekilde düzenleyelim. Bu r nesnenin toplam düzeninin sayısı t olsun. Eğer bütün nesneler farklı olsalardı, böyle bir düzenlemenin sayısı (r!) kadar olacaktı. Bu durumda,toplam düzenleme sayısı (t)(r!) kadardır. Fakat nesneler farklı olduğu durumda toplam düzenleme P(n,r) dir. Böylece t=P(n,r)/(r!) = C(n,r) bulunur.

Örnek: Pul defterinde pul koymak için beş yer kalmış ise elimizde bulunan sekiz adet pulu kaç farklı şekilde yerleştirebiliriz.

Çözüm: C(8,5)= 8!/5!(8-5)! = 8!/(5!3!) = 56.

Teorem: Pascal Formülü:

C(n,r)= C(n-1,r) + C(n-1,r-1) dir.

İspat:

X, n elemanlı küme ve Y, X'in (n-1) elemanlı alt kümesi olsun. X'te olan fakat Y'de olmayan bir t elemanı alınsın.X'in her bir r elemanlı alt kümesi, ya Y'nin r-elemanlı alt kümesi veya, Y'nin (r-1) elemanlı alt kümesi ile t'yi içeren tek elemanlı kümenin birleşimi olan kümedir. Önceki kategoride C(n-1,r) küme vardı ve sonra C(n-1,r-1) küme vardır. Diğer bir deyimle, X'in r elemanlı alt kümelerinin toplamı,C(n-1,r)+C(n-1,r-1) 'e eşittir.

Genelleştirilmiş Kombinasyon

k farklı gruba ait olan n nesnenin düzeni ele alınırsa; 1. Gruba ait olan n_1 benzer nesnenin n konuma koyulması $C(n,n_1)$ şekilde,sonraki gruptaki n_2 nesne $C(n-n_1, n_2)$ şekilde yerleştirilebilir. Devam edilerek çarpma kuralına göre toplam sayı;

$C(n;n_1,n_2,..,n_k) = C(n,n_1)\ C(n-n_1,n_2).C(n-n_1-n_2,n_3)\ldots\ldots\ldots\ldots\ldots C(n-n_1-n_2--\ldots\ldots\ldots-n_{k-1},n_k)$ olarak bulunur.

Teorem: $n_1+n_2+..+n_k \leq n$ olmak üzere $P(n;n_1,n_2,..,n_k) = C(n;n_1,n_2,..,n_k) = (n!)/(n_1)!(n_2)!..(n_k)!$ dir.

Özellik:C(n;r)=C(n;n-r)=C(n;r,n-r)

Örnek:

P(15;3,5,7,)=(15!)/(3!)(5!)(7!) =P(15,8)/(3!)(5!)=P(15;3,5)/(7!)

C(15;3,5,7)=C(15,3)C(12,5)C(7,7)=C(15,3)C(12,5)=C(15;3,5) /(7!)

Sonuçta: $C(15;3,5,7) = \dfrac{(15!)}{(3!)(5!)(7!)} = P(15;3,5,7)$ bulunur.

Teorem: (multinomial th.) $(x_1+x_2+\ldots\ldots\ldots+x_k)^n$ nın açılımında $x_i(i=1,2,,\ldots.,n)$ n_i (burada $n_1+n_2+\ldots\ldots.n_k=n$) kere bulunur ve terimlerin katsayısı $C(n;n_1,n_2,\ldots,n_k)$ ile hesaplanır.

Örnek: $(a+b+c+d)^{15}$ 'in açılımında $a^3b^2c^6d^4$'ün katsayısı (15!)/(3!)(2!)(6!)(4!) dür.

Örnek: Binom Teoremi; Multinomial teoremi k=2 olduğunda Binom teoremi adını alır ve aşağıdaki şekilde ifade edilir.

$(x+y)^n = \Sigma C(n,n-r)\ x^{n-r}y^r$ ile hesaplanır.

Bir kümenin Bölmelenmesi:

n elemanlı Bir kümenin, her birsi n_i (i=1,2,….,k) elemanlı p_i alt kümeye bölmelenmesi problemi için bölmeleme sayısı;

$$\frac{(n!)}{(p_1!)(n_1!)^{p1}(p_2!)(n_2!)^{p2}....(p_k!)(n_k!)^{pk}}$$ ile hesaplanır

Örnek: 43 adet öğrenciyi, 7 farklı yatakhaneye, ilk iki gruba 5 öğr. Sonraki üç gruba 6 ve 6.ya 7, yedinciye ise 8 öğrenci kaç şekilde yerleştirilebilir?

Çözüm: $\dfrac{(43!)}{(2!)(5!)(5!).(3!)(6!)(6!)(6!).(7!)(8!)}$

Eğer X, n elemanlı küme ise, X'in r-permutasyonu, X'in tekrarlanmayan elemanlarının düzenidir. Benzer şekilde,r-kombinasyon ise,X'ten tekrarlanmayan r eleman seçilmesidir.Her iki durumda da r, n'den büyük olamaz. Eğer tekrarlamaya müsaade edilirse, bu durumda r, n'i geçebilir.

Tanım; X, n elemanlı bir küme ise, X'in r-sekansı,elemanların tekrarlanabildiği r elemanın düzenidir. Çarpma kuralının basit bir uygulaması olarak, n elemanlı bir kümedeki r-sekansın sayısı $\mathbf{n^r}$ kadardır. Herhangi bir r-permutasyonun r-sekans olduğu açıktır. Diğer taraftan farklı elemanlı r-sekans bir r-permutasyondur. Örn. aabdac ve aadbac , X={a,b,c,d} kümesinden seçilen 6'lı sekansıdır.

n elemanlı X kümesinden seçilen r nesnenin koleksiyonu(farklı olması gerekli değil) X'ten r-koleksiyon olarak adlandırılır. r-sekansın tersine, r-koleksiyonda, seçilen elemanların sırası önemli değildir. Örn. [a,a,b,c]'nin 4 koleksiyonu ile [a,b,c,a]'nın 4 koleksiyonu arasında fark yoktur.

Verilen bir n elemanlı kümeden tekrarlanabilen r tane eleman kaç farklı şeklide seçilebilir. Sorunun cevabı aşağıdaki teorem ile verilebilir.

Teorem(ispatsız): X, kardinalitesi n olan bir küme olsun. X'ten alınacak r koleksiyonun sayısı L= C(r+n-1,n-1)=C(r+n-1,r) kadardır.

r benzer nesnenin n farklı konuma yerleştirilmesinin sayısı M= C(r+n-1,n-1) kadardır.

$x_1+x_2+\ldots+x_n=r$ denkleminin pozitif tamsayılardaki çözümünün sayısı N=C(r+n-1,n-1) kadardır

Örnek: X={a,b,c,d} kümesinden 5'li koleksiyonların sayısı C(5+4-1,4-1)=56'dır hâlbuki aynı kümeden seçilen 5'li sekansların sayısı $4^5 = 1024$ Dür.

N farklı elemanlı kümenin r elemanının Permutasyon ve kombinezonları 4 farklı durumu için tekrarlamalı ve tekrarsız olarak anlatılanlar aşağıdaki şekilde özetlenebilir.

Tablo Farklı permutasyon ve Kombinezon Modeli

	Seçme Modeli n elemanlı X Kümesinden r elemanın seçiminin miktarı	Tahsis Modeli n farklı konumlu X kümesinin konumlarına r nesnenin bir koleksiyonunun tahsisinin miktarı
P(n,r)	Seçilen elemanlar farklı ve sıraları önemli	Nesneler farklı ve bir konum birden fazla nesne alamaz.
C(n,r)	Seçilen elemanlar farklı ve sıraları önemli değil	Nesneler aynı olabilir ve bir konum birden fazla nesne alamaz.
n^r	Seçilen elemanlar farklı olmayabilir (tekrarlanabilir) ve sıraları önemli	Nesneler farklı ve bir konum birden fazla nesne alabilir.
C(r+n-1,n-1	Seçilen elemanlar farklı olmayabilir (tekrarlanabilir)ve sıraları önemli değil	Nesneler aynı ve bir konum birden fazla nesne alabilir.

Güvercin yuvası(Pigeonhole) prensibi

Basit ve açık bir prensip olan güvercin yuvası prensibi, kombinatorik teoride oldukça çok kullanılır. Güvercin yuvası problemine en fazla bilgisayar bilimlerinde karşılaşılır. Örneğin, olası anahtar sayısı dizideki indis sayısını geçtiği için çarpışmalar özet fonksiyonlarında kaçınılmazdır. Bu çarpışmalardan kaçınabilen akıllı bir özet fonksiyonu yoktur. Bu prensip aynı zamanda en az bir dosyayı kısaltırken diğer bir dosyayı uzatan kayıpsız sıkıştırma algoritmasını sağlar.

10 fakülte elemanının yerleşeceği 9 oda olduğu durum da yerleşim, 19 fakülte elemanının olduğu durumdaki oda paylaşımı vs. gibi durumlardaki çözümler güvercin yuvası prensibi ile bulunur.

Prensip basit şekliyle, Dirichlet güvercin yuvası prensibi olarak bilinir ve eğer n+1 güvercin n adet yuvaya yerleştirilecek olursa en az bir yuvada birden fazla güvercin olacaktır. Tersi eğer n güvercin n+1 yuvaya koyulacak olursa en az bir yuva boş kalacaktır.

Prensibin daha genel hali ise, eğer k.n+1 veya daha fazla güvercin, n yuvaya koyulacak olursa, en az bir yuvada k dan fazla güvercin olacaktır.

Örnek: Bir kampüste 18 adet oturma salonu bulunmaktadır. Öğrenci dekanı, bir salondaki bilgisayar kullanımını anlamak için anket yapmak amacıyla seçeceği salondan 5 kişilik öğrenci komitesi oluşturmak ister ve salonlara duyurular asar. En az kaç kişi bu ankete cevap vermelidir ki, dekan bir salon seçip komite oluşturabilsin.

Çözüm: Genel güvercin yuvası prensibi gereği, k=4 olur ve k.n+1 = 4.18 +1= 73

Tanım: Eğer, m ve n pozitif tamsayılar ise, m/n'in tabanı, m/n'e eşit veya küçük en büyük tamsayıdır ve m/n'in tavanı, m/n'e eşit veya büyük olan en küçük tamsayıdır. (Örnek. 38/9'un tabanı 4 tavanı ise 5 'dir.)

Teorem: a) Eğer m güvercin n yuvaya yerleştirilirse, en az bir yuvadaki güvercin sayısı k'dan fazla olacaktır, burada k=taban [(m-1)/n]dir.

b) Eğer, $m=p_1+p_2+\dots\dots+p_n$ - n+1 (her bir p_i bir pozitif tamsayı) güvercin, n adet yuvaya tahsis edilirse, ilk yuvada en az p_1 adet güvercin veya ikinci de en az p_2 adet güvercin ….. veya n'inci de p_n adet güvercin bulunur.

İspat:

a) k'dan.(n).(k) ≤ (m-1) < m dir. Eğer güvercin sayısı tam olarak k.n ise, her bir yuvaya k adet güvercin koymak mümkündür. Fakat güvercin sayısı k.n 'den büyük olan m'e eşit isen az bir yuvada k'dan fazla sakin olacaktır.
b) Burada, k= taban[$(p_1+p_2+\dots\dots+p_n)$/n]-1 dir. Böylece, (k+1), n tamsayının en az birisine eşit veya büyüktür.

Örnek: Bir çantada,tam olarak 6 kırmızı,5 beyaz ve 7 mavi bilya bulunmaktadır.Seçilen bilyalar içinden ya en az 3 kırmızı veya en az 4 beyaz veya en az 5 mavi bilya olması için kaç bilya seçilmelidir.

Çözüm: 1.yol önceki teoreme göre, burada n=3, p_1 = 3, p_2=4 ve p_3=5 dir. Böylece, m=(3+4+5)-3+1 = 10'dur.

2. yol: kırmızı, beyaz ve mavi bilyalar sırasıyla x,y,z olsunlar. Bunun için x en az 3

veya y en az 4 veya z en az 5 olmalıdır.Eğer, x en fazla 2, y en fazla 3 ve z en fazla 4 olursa $x+y+z = 9$ olur ve bu durum gerçekleşmez. Öyleyse en az 10 adet bilya seçilmelidir.

Teorem : $X=\{1,2,3,\ldots,2n\}$ ve X'in (n+1) elemanlı alt kümesi S verilsin. S'de birbirini bölen en az iki sayı vardır.

İspat: S'deki herhangi bir sayı $r= 2^t.s$ ($t \geq 0$ olan tamsayı) ve r'nin tek parçası denilen s, X'ten bir tek sayı olarak yazılabilir. X'te n adet tek sayı olduğundan s için en fazla n seçim vardır. n tek parça, n güvercin yuvası olarak düşünülebilir ve S'nin (n+1) sayısı buraya yerleştirilebilir. Diğer bir ifade ile, S'de aynı tek parçaya sahip $x= 2^t.s$ ve $y= 2^u.s$ olsun. Burada ya x, y'yi böler veya y, x'i böler.

Teorem: (n^2+1) farklı sayının herhangi sekansı, ya artan ya da azalan sırada olan en az (n+1) elemanlı bir alt sekans içerir.

İspat: sekans $a_i(i=1,2,\ldots,n^2+1)$ ve a_i'den başlayan artan sıradaki sekansların en büyüğündeki terim sayısı t_i olsun. Eğer bazı i'ler için $t_i=n+1$ ise tamam.

$\forall i$ için, $t_i \leq n$ olsun. $H_j=\{a_i: t_i=j\}$ olsun. Burada $j=1,2,,\ldots,n$ dir. Böylece, (n^2+1) sayıda t_i'yi koyabileceğimiz $H_1,H_2,\ldots,H_n$ olmak üzere n adet güvercin yuvamız olmuş olur. Böylece genelleştirilmiş güvercin yuvası prensibine göre, bu sayılardan k = taban($[(n^2+1)-1]/n =n$) tanesinden fazlasını alabilen bir H_r güvercin yuvası vardır. Böylece t_i sayıları arasında, onların en az birisi (n+1) e eşittir.

Şimdi sekanstaki (n+1) elemana karşılık gelen H_r güvercin yuvasındaki sayıların azalan sırada bir dizi oluşturduğunu gösterelim.

$i <j$ olmak üzere a_i ve a_j nin H_r içinde olduğunu kabul edelim. Sekans içindeki elemanlar farklı olduğu için ya $a_i<a_j$ ya da $a_i>a_j$ dir. Şimdi, $a_i<a_j$ olduğunu kabul edelim, o halde, $a_j \in H_r$ demek a_j'den başlayan ve uzunluğu r olan bir alt sekans var demektir. Oysa, $a_i<a_j$ demek a_i'den başlayan (r+1) uzunluğunda bir alt sekans olduğu anlamına gelir. Bu bir çelişkidir, çünkü a_i, H_r'nin elemanı olduğu için, a_i'den başlayan (r+1) uzunluğunda bir alt sekans olamaz. Böylece, i<j olsa da, $a_i>a_j$ dir. Böylece H_r'deki herhangi (n+1) eleman azalan sırada bir alt sekans oluşturur.

Örnek: Yukarıdaki teoremi aşağıda verilen diziler için uygulayalım.

a) 15,12,5,7,9,6,3,4,10,14

b) 15,12,9,10,7,5,4,14,3,6

Çözüm a) burada dizide 10 eleman olduğu için n=3'dür ve bunlara karşı gelen t_i'ler, 1,2,5,4,3,3,4,3,2,1 dir. t_3 =5 olduğu için a_3'ten başlayan 5 elemanın artan sırada oluşturduğu dizi 5,7,9,10,14 dir.

b) Burada uygun t_i: 1,2,3,2,2,2,2,1,2,1 dir. Hiçbirisi 3'den fazla değildir. $H_1=\{15,14,6\}$, $H_2=\{12,10,7,4,3\}$ ve $H_3=\{9,5\}$'i alalım. k'inci kümedeki oluşan sıra 5 elemanlı azalan bir dizidir.

2.4 Ekleme Çıkarma Prensibi(Inclusion-Exclusion Principle)

Bazı kompleks matematiksel sonuçlar sayma argümanlarının ispatlarına bağlıdır: çeşitli kümelerin eleman sayılarını saymak, belli bir sonucun kaç değişik yolla elde edilebileceğini saymak gibi. Sayma kısmen kolay bir olay gibi görünse de, pratikte çok kompleks olabilir. Matematikçiler sayma problemleri için birçok teknik ve sonuç üretmişlerdir ve konuya sayma teorisi adını vermişlerdir.

Saymanın en basit sonuçlarından biri şudur: iki ayrık A ve B kümesinin toplam eleman sayısını

bulmak için A'nın elemanlarını, B'nin elemanlarını sayıp toplarız. Burada | A| A kümesinin eleman sayısını gösterir.(Bazen N(A) olarak gösterilir)

Sayma Prensibi 1: Eğer A ve B ayrık iki küme ise $|A \cup B| = |A| + |B|$.

Çoğu uygulama doğal olarak ikiden fazla küme içerir. Yukarıdaki prensip aşağıdaki şekilde genelleştirilir.

Sayma Prensibi 2: Eğer $A_1, A_2, \ldots, A_n$ küme ise ve bu kümelerin hiçbir çifti ortak bir elemana sahip değilse $| A_1 \cup A_2 \cup \ldots \cup A_n | = |A_1|+|A_2|+\ldots+|A_n|$.

Bazen, elemanları sayılacak kümeler yukarıdaki sayma prensiplerinin katı kuralını-herhangi bir çiftin ayrık olması sağlamayabilir. Öte yandan, bu durumda kümeyi sayma prensiplerinin koşullarını sağlayacak alt kümeler bölmek mümkündür. Bu şekilde ispatlanabilecek en basit sonuç şudur:

Teorem 1.2(Ekleme(inclusion)-Çıkarma(exclusion) Prensibi): Eğer A ve B sonlu kümeler ise $|A \cup B|=|A|+|B|-|A \cap B|$.

İspat: $A \cup B$' yi sayma prensibi 2'yi sağlayan alt kümelerine böleriz: A-B, $A \cap B$ ve B-A.

Sayma prensibi 2' den,

$$| A \cup B | = |A-B|+| A \cap B |+|B-A|. \qquad (1)$$

A ve B kümelerinin kendileri sırasıyla A-B, $A \cap B$ ve B-A, $A \cap B$ şeklinde ayrık alt kümelere bölünebilir. Böylece;

$$|A|=|A-B|+| A \cap B | \qquad (2)$$

$$|B|=|B-A|+| A \cap B |. \qquad (3)$$

Bu durumda (1), (2) ve (3) eşitliklerini birleştirerek istenilen sonucu elde etmek çok kolay bir işlemdir. Ekleme-çıkarma prensibi bu şekilde adlandırılır çünkü $A \cup B$' nin elemanlarını saymak için A'nın elemanlarını ve B'nin elemanlarını ekledik ve böylece $A \cap B$' nin elemanlarını iki kere eklemiş olduk. $A \cup B$' nin doğru eleman sayısını elde etmek için $A \cap B$'yi bir kere çıkarmamız gerekir.

İki kümeden fazla durumlar için benzer sayma teknikleri vardır. Üç küme için sonuç aşağıdaki teoremdeki gibi bulunur.

Teorem 1.3: A, B ve C sonlu kümeler ise

$$|A \cup B \cup C|=|A|+|B|+|C|-| A \cap B |-| B \cap C |-| C \cap A |+|A \cap B \cap C|.$$

Genel durumda ekleme- çıkarma prensibi, n adet farklı küme A_i için;

$$|A_1 \cup A_2 \cup \ldots \cup A_n|= \sum_{1 \le i \le n} | A_i | - \sum_{1 \le i < j \le n} | A_i \cap A_j | + \sum_{1 \le i < j < k \le n} | A_i \cap A_j \cap A_k | - \ldots + (-1)^{n+1} |A_1 \cap A_2 \cap \ldots \cap A_n|$$

dir.

İsp: Birleşimdeki bir elemanın, eşitliğin sağ tarafında bir kere sayıldığını göstererek ispatı yapacağız. $1 \le r \le n$ olmak üzere, a, $A_1, A_2, \ldots A_n$ kümesinden r tanesinin tam olarak bir elemanı

olsun. Bu eleman $\Sigma|A_i|$ ile C(r,1) kere sayılır. Aynı eleman $\Sigma|A_i \cap A_j|$ ile C(r,2) kere sayılır. Eleman genel olarak m içeren A_i kümelerinde C(r,m) kere sayılır. Böylece eleman tam olarak eşitliğin sağ tarafında,

C(r,1)-C(r,2)+C(r,3)-……+$(-1)^{r+1}$C(r,r) defa sayılır , $\sum_{k=0}^{n}(-1)^k C(n,k)=0$ eşitliğinden

C(r,0) -C(r,1)+C(r,2)-……+$(-1)^{r}$C(r,r) =0 yazılabilir. Buradan,

1=C(r,0)= C(r,1)-C(r,2)+……+$(-1)^{r+1}$C(r,r) dir. Böylece, birleşimdeki her eleman ifadenin sağ tarafında tam olarak bir kere sayılmış olur. Bu ekleme-çıkarma prensibinin ispatıdır.

Ekleme-Çıkarma prensibine alternatif tanım

N elemanlı X kümesinin bütün sonlu alt kümelerini düşünelim. Eğer A, X'in alt kümesi ise A'nın tümleyeni $\overline{A}$ ile gösterilir. N(X), X'deki elman sayısını gösterir. Buradan, $\overline{A} = X - A$ böylece;

i) N($\overline{A}$) = N- N(A) dir. (X'te bulunan herhangi bir alt küme A için)

A ve B, X'in iki alt kümesi olsunlar. Buradan i) kullanılarak N($\overline{A \cup B}$) = N- N(A∪B) dir. Burada, ekleme çıkarma prensibi gereği N(A∪B) =N(A) +N(B) –N(A∩B) dir. Aynı zamanda $\overline{A \cup B} = \overline{A} \cap \overline{B}$ 'dir. Böylece;

ii) N($\overline{A} \cap \overline{B}$) = N –N(A)-N(B) +N (A∩B) dir. Benzer şekilde;
iii) N($\overline{A} \cap \overline{B} \cap \overline{C}$) = N- N(A)-N(B)-N(C) + N(A∩B) + N(A∩C)+N(B∩C)- N(A∩B∩C) dir.

(i),(ii) ve(iii) ifadeleri, N elemanlı kümenin bir altkümesi, iki alt kümesi ve üç alt kümesini içeren ekleme çıkarma kuralının uygulaması olarak düşünülebilir.

Şimdi a_i(i=1,2,3) , X kümesinin elemanları ile birlikte verilen üç farklı özellik olsun, öyle ki tipik bir eleman bu özelliklerin bir veya daha fazlasını alabilir veya hiçbirini almayabilir. A_i ,X'deki özelliği a_i olan x'lerin kümesi olsun. N(a_i) , X'deki özelliği a_i olan elemanların sayısı, N(a'_i) ise, X'de özelliği a_i olmayan elemanların sayısı, ve N(a_1,a_2) ise, X'de özelliği a_1 ve a_2 olan elemanların sayısı olsun ve diğerleri benzer şekilde belirlensin. Buradan, N(a_i)=N(A_i), N(a_i,a_j)= N($A_i \cap A_j$) ve N(a_i,a'_j)= N($A_i \cap \overline{A}_j$) dir. Ekleme çıkarma kuralı (iii) yukarıda verilenler cinsinden yeniden yazılırsa:

N(a'_1,a'_2,a'_3)=N-[N(a_1)+N(a_2)+N(a_3)]+[N(a_1,a_2)+N(a_1,a_3)+N(a_2,a_3)]- N(a_1,a_2,a_3)

Bu sonuç n farklı özelliği içerecek şekildeki durum için genişletilebilir. Bundan önce aşağıdaki notasyonu açıklayalım. Daha genel bir ifade ile, A_i 'ler(i=1,2,….n olmak üzere) X'in n adet alt kümeleri olsunlar. Bir k elemanlı kesişim, bu n küme arasındaki farklı herhangi k tanesinin kesişimidir. k- elemanlı kesişimin sayısı C(n,k) dır. S_k bütün k elemanlı kesişimlerdeki eleman sayısı olmak üzere;

S_1=N(A_1)+N(A_2)+ …….N(A_n)= $\sum_{1 \le i \le n} |A_i|$;

S_2= N($A_1 \cap A_2$)+N($A_1 \cap A_3$)+ …….N($A_{n-1} \cap A_n$)= $\sum_{1 \le i < j \le n} |A_i \cap A_j|$,

diğer elemanlar için devam edilirse; N , X ‘in eleman sayısı olmak üzere

$N(\overline{A_1} \cap \overline{A_2} \cap_{...} \cap \overline{A_n})$= N- S_1 +S_2-…..$(-1)^n S_n$ şeklinde de ifade edilebilir.

Örnek: Birinci sınıf yatakhanesindeki her bir öğrenci, dört giriş dersi(Biyoloji(B), İngilizce(I), Tarih(T),Matematik(M))’nden en az birini almaktadırlar. Bütün dersleri 6 öğrenci almaktadır. 25 öğrenci bir adet ders, 15 öğrenci derslerden herhangi ikisini, 10 öğrenci ise, derslerden herhangi üçünü almaktadır. Yatakhanede kaç öğrenci vardır?

Çözüm: Öğrenci sayısını N ile gösterelim. Buradan. S1=C(4,1).(25)= 100 ; S2= C(4,2).(15)=90; S3=C(4,3).(10)= 40; S4=C(4,4)(6) =6 dır. Her bir öğrenci en az bir ders aldığı için,

$N(\overline{B} \cap \overline{I} \cap \overline{T} \cap \overline{M})$ =0 dır. Buradan ekleme çıkarma kuralına göre;

0= N- S_1+S_2-S_3+S_4= N-100+90-40+6 N=44 bulunur.

Düzensizlik(Derangements) : Ekleme- çıkarma prensibi, hiçbir nesnenin kendi asıl yerinde olmadığı n nesnenin permutasyonunu saymakta kullanılır.

Örnek: 21453, 12345’in bir düzensizliğidir. Çünkü hiçbir eleman kendi asıl yerinde değildir. Hâlbuki, 21543 , 12345’in bir düzensizliği değildir. Çünkü, 4 kendi asıl yerindedir.

Teorem: n elemanlı bir kümenin düzensiz permutasyonun sayısı;

D_n = n![1-1/(1!)+ 1/(2!)- 1/(3!)+….+$(-1)^n$. 1/(n!)] ile hesaplanır.

İspat: N, X üzerinde toplam permutasyon sayısı ve A_i’de i. Nesnenin yerinde olduğu permutasyonların kümesi olsun. X’deki toplam permutasyon sayısı n! dir. Böylece; D_n =n!-S_1+S_2+…$(-1)^n S_n$ dir. Burada;

S_1= C(n,1)(n-1)!

S_2= C(n,2)(n-2)!

.

S_k= C(n,k)(n-k)! Devam edilir.

Böylece: D_n= n![1-1/(1!)+ 1/(2!)- 1/(3!)+….+$(-1)^n$. 1/(n!)] bulunur. Ekleme-Çıkarma prensibi kullanılarak, bir sonlu kümenin r-sırasının sayısını ve kümenin bölmeleme sayısını bulmak mümkündür.

İkinci tür stirling sayıları

S(r,n) stirling sayısı, r elemanlı bir kümeyi, boş olmayan n gruba parçalama yollarının sayısıdır.

$S(r,n) = (n^r - C(n,1)(n-1)^r + C(n,2)(n-2)^r - ... + (-1)^{n-1}C(n,n-1)1^r)/(n!) = \frac{1}{n!}\sum_{i=0}^{n-1}(-1)^i C(n,i)(n-i)^r$

$r,n \in \boldsymbol{N}$, $1 \le n \le r$

$(n!)S(r,n) = n^r - C(n,1)(n-1)^r + C(n,2)(n-2)^r - …… + (-1)^{n-1}C(n,n-1)1^r$ dir.

Teorem: a) Yerleştirme problemi: r farklı nesnenin n farklı konuma her bir konum en az bir eleman alacak şekilde yerleştirme sayısı (n!)S(r,n)‘dir.

b) Küme bölmeleme problemi: Kardinalitesi r olan kümenin n boş olmayan kümeye bölmelenmesinin sayısı S(r,n) ve r elemanlı bir kümenin en çok n boş olmayan kümeye bölmelenme sayısı S(r,n)+S(r,n-1)+…+S(r,1) tanedir.

Örnek: S(4,2) =(2^4- C(2,1)$(2-1)^4$)/2!= (16-2)/2=7 dir. Çünkü dört nesneye sahip bir küme iki alt

kümeye 7 şekilde bölmelenebilir. Küme {a,b,c,d} olsun. Aşağıdaki şekilde alt kümelere bölmelenebilir.

{a}{b,c,d}, {b}{a,c,d},{c}{a,b,d},{d}{b,c,a},{a,b}{c,d},{a,c}{b,d},{a,d}{b,c}

Sonlu bir kümeden sonlu bir kümeye olan fonksiyonların sayısı.

X ve Y, sırayla kardinalitesi r ve n olan iki sonlu küme olsunlar. X'ten Y'ye herhangi keyfi bir fonksiyon ***f*** olsun. X'teki herhangi r eleman, Y 'deki n elemandan birisine n yol ile dönüştürülebilir. Böylece çarpma kuralı gereği X'ten Y'ye n^r adet fonksiyon vardır. Fakat eğer ***f*** birebir fonksiyon(injeksiyon) ise r elemanın dönüşebileceği yol sayısı daha az olacaktır ve gerçekte, n(n-1)(n-2)……(n-r+1) adet olacaktır. Eğer dönüşüm bir örten fonksiyon(surjeksiyon) ise Y'deki her elemanın bir ön görüntüsü vardır. Örten fonksiyon sayısı ise, n^r-C(n,1)$(n-1)^r$ + C(n,2)$(n-2)^r$-……+$(-1)^{n-1}$C(n,n-1)1^r ile hesaplanır. Bu anlatılanlar aşağıdaki teorem ile özetlenebilir.

Teorem: X ve Y, sırayla kardinalitesi r ve n olan iki sonlu küme olsunlar. 1) X'ten Y'ye olan fonksiyon sayısı $\mathbf{n^r}$, 2) X'ten Y'ye olan birebir fonksiyon sayısı P(n,r), 3) X'ten Y'ye olan örten fonksiyon sayısı ise n^r-C(n,1)$(n-1)^r$ + C(n,2)$(n-2)^r$-……+$(-1)^{n-1}$C(n,n-1)1^r kadardır.

Örnek: Beş farklı iş dört farklı çalışana, her birine en az bir iş verilecek şekilde kaç türlü dağıtılabilir?

Çözüm: İş dağıtımını, beş iş türü içeren kümeden dört işçi içeren kümeye fonksiyon olarak ele alırsak: Bir dağıtım, her işçiye en az bir iş verilecek şekilde olursa, iş kümesinden işçi kümesine olan örten fonksiyon ile aynı olacaktır. Yukarıdaki teoremden; 4^5-C(4,1)3^5+C(4,2)2^5-C(4,3)1^5=1024-972+192-4=240 farklı şekil bulunur.

3 Üretken Fonksiyonlar

Üretken fonksiyonlar, kabaca diziliş problemlerini fonksiyonlara dönüştürürler. Bu özelliği ile diziliş konusundaki tüm problemleri bu yapıya uygulayabiliriz. Bu yol ile sayma problemlerinin çözümü için üretken fonksiyonlar kullanılabilir. Tipik bir problem olarak 62 cent oluşturmak için kullanılacak çeyrek(25 cent),dimes(10 cent), nickels(5 cent) ve 1 cent sayısı ne olmalıdır? Çözüm pozitif sayılarla ve q+d+n+c=62 olacaktır. Burada, q, Q={0,25,50} kümesinden; d, D={0,10,20,30,40,50,60} kümesinden; n, N={0,5,10,15,20,25,…,65} kümesinden ve c, C={0,1,2,……..60,61,62} kümesinden seçilecektir. Bu bozukluk oluşturma problemini çözmek için üretken fonksiyonları kullanarak bir çözüm üretmek gereklidir. Daha basit bir problem örneği verelim.

Örnek: a+b+c =10 denkleminin her bir değişkenin en az 2 en fazla 4 olduğu tamsayı çözümü kaç tanedir?
Çözüm: Aşağıdaki tablo oluşturulduğunda problem için 6 farklı çözüm olduğu görülür.

a	b	c
2	4	4
3	4	3
3	3	4
4	2	4
4	4	2
4	3	3

Şimdi her bir değişken için p_a,p_b, ve p_c olan üç polinom tanımlayalım. Her bir değişkenin değeri 2,3 veya 4 olabileceği için her polinom $x^2+x^3+x^4$ olarak tanımlanır ve bu üç polinom, üsleri 6 ila 12 arasında olan x'leri içeren p(x) polinomunu elde etmek için çarpılırlar. P(x) bir üretken fonksiyon örneğidir. Şimdi, a+b+c=10 olduğu için $p(x) = (x^2+x^3+x^4)^3$ polinomunda x^{10} teriminin katsayısının kaç farklı şekilde oluşturulabileceğinin çözümü yapılırsa; p_a dan x^2, p_b'den x^3 ve p_c 'den x^4 alınır. Problemin her bir çözümü bir farklı yol olduğu için 6 farklı yol vardır.

Tanımlar: (a) Bir kuvvet serisi $a_0+a_1x+a_2x^2+a_3x^3+\ldots$ Şeklinde olan sonsuz bir seridir. Burada, $a_i(i=0,1,2,\ldots)$ gerçel sayı ve x bir değişkendir.

(b) Eğer $a_0+a_1x+a_2x^2+a_3x^3+\ldots$ ve $b_0+b_1x+b_2x^2+b_3x^3+\ldots$ iki kuvvet serisi iseler, bunların toplamı da kuvvet serisidir ve x_r 'nin katsayısı a_r+b_r 'dir ve bu kuvvet serilerinin çarpımı da kuvvet serisidir ve x_r 'nin katsayısı, $(a_0b_r+a_1b_{r-1}+a_2b_{r-2}+\ldots+a_rb_0)$ dır.

(c) Eğer $a_r(r=0,1,2,\ldots)$, belirli bir kombinezonsal problemde r nesneyi seçme şeklinin sayısı ise, bu problem için sıradan üretken fonksiyon $a_0+a_1x+a_2x^2+a_3x^3+\ldots$ şeklindeki kuvvet serisidir.

x'in herhangi bir polinomu x'in kuvvet serisidir. Örneğin, $3x^2+2x^4$, $0+0.x+3.x^2+0.x^3+2.x^4+0.x^5+0.x^6+\ldots$ olarak yazılabilir.
Şimdi a+b+c=r olan problemi düşünelim. Burada, a,b, ve c en az 2 en fazla 4 olacaktır. Buradan r 6 ile 12 arasında değişir. Sabit bir r için a_r tamsayı çözümlerin sayısıdır.Buradan a_r , $g(x)= (x^2+x^3+x^4)^3 = x^6+3x^2+6x^8+7x^9+6x^{10}+3x^{11}+x^{12}$ olan üretken fonksiyonunda x^r'nin katsayısıdır.

Örnek: n elemanlı bir kümeden r elemanın seçilme sayısı, C(n,r) dir ve bu kombinasyonel problem için üretken fonksiyon g(x) dir. Burada;
$(1+x)^n$'in binom açılımı olan $g(x) = c(n,0)+C(n,1)x+C(n,2)x^2+\ldots+C(n,r)x^r+\ldots+C(n,n)x^n$ fonksiyonudur.

3.1 Sıradan üretken Fonksiyonlar

$a_0,a_1,a_2,a_3,\ldots$ şeklindeki sonlu sekanslar için sıradan üretken fonksiyonlar biçimsel kuvvet serileridir: $g(x)= a_0+a_1x+a_2x^2+ a_3x^3\ldots$

Bir üretken fonksiyon, genellikle x'in bir sayı yerine yer belirleyici olduğunun kabul edildiği bir biçimsel kuvvet serisidir. Üretken fonksiyonların katsayılarının hesabının yapılması önemlidir. Bu bölümde katsayıların hesabı için geliştirilen yöntemler açıklanmıştır.

Teorem:
(a) $g(x)= (1+x+x^2+x^3+\ldots)^n$ fonksiyonunda, x^r'nin katsayısı a_r olsun, $a_r=C(r+n-1,r)$ ile hesaplanır.
(b) $(1-x^m)^n=1-C(n,1)x^m+C(n,2)x^{2m}-\ldots+(-1)^nx^{nm}$ dir
(c) $(1+x+x^2+ \ldots+x^{m-1})^n.= (1-x^m)^n(1+x+x^2+ \ldots)^n$ dir.

İspat: (a) g(x) bir üretken fonksiyondur ve $y_1+y_2+\ldots.+y_n=r$ denkleminin pozitif tamsayılardaki çözümünün sayısı a_r, C(n+r-1,n-1) ile bulunuyordu(Bölüm 2'de verilen teorem) Bu sonuç C(r+n-1,r) ile aynıdır. (Kombinezon özelliği)
(b) Binom ifadesinde $(1+t)^n$, $t=(-x^m)$ koyulursa bu açılım elde edilir.
(c) $1+x+x^2+ \ldots+x^{m-1}.= (1-x^m)(1+x+x^2+ \ldots)$ eşitliğinin her iki tarafının n. kuvveti alınarak kolayca ispatlanır.

Örnek: a+b+c+d=27 denklemini tamsayı çözümlerinin sayısını bulun. Burada her değişken en az 3 en fazla 8 değerini alacaktır.

Çözüm: $g(x)= (x^3+x^4+\ldots+x^8)^4$ de x'in 27. kuvvetinin katsayısı çözümün sayısıdır ve bu sayı $h(x)= (1+x+\ldots.+x^5)^4$'deki x'in 15. kuvvetinin katsayısıdır. Yukarıdaki teoremin c şıkkından,
$h(x)=(1-x^6)^4 (1+x+ x^2\ldots.)^4$ dir.

$(1-x^6)^4 = 1-C(4,1)x^6+C(4,2)x^{12}+\ldots$ (Teoremin b şıkkından.)
Aynı teoremin a şıkkından,
$(1+x+ x^2\ldots.)^4 = 1+C(4,1)x +C(5,2)x^2+C(6,3)x^3 +\ldots..$
Böylece h(x)'deki x'in 15. kuvvetinin katsayısı , C(18,15)-C(4,1)C(12,9) +C(4,2)C(6,3) = 56 dir.
Eğer, $a_0+a_1x+a_2x^2+ \ldots+ a_rx^r +\ldots.$ Bir g(x) fonksiyonunun kuvvet serisi açılımı ise, g(x), a_r dizisi için bir üretken fonksiyondur. Verilen bir üretken fonksiyondan farklı a_r katsayılarına sahip yeni bir üretken fonksiyon oluşturmak mümkündür. Bu özellik aşağıdaki ispatsız teorem ile belirtilmiştir.

Teorem: Eğer a_r için g(x), b_r için de h(x) üretken fonksiyonlar ise;
(a) $A.a_r+B.b_r$ için üretken fonksiyon A.g(x) +B.h(x) dir.
(b) a_r-a_{r-1} için üretken fonksiyon (1-x)g(x) dir.
(c) $(a_0+a_1+a_2+\ldots+ a_r)$ için üretken fonksiyon, $(1+x+ x^2\ldots.)g(x)$ dir.
(d) $(a_0b_r+a_1 b_{r-1} +a_2 b_{r-2} +\ldots+ a_rb_0)$ için üretken fonksiyon, g(x)h(x) dir.
(e) ra_r için üretken fonksiyon, x.g'(x) dir. Burada g'(x), g(x) in x'e göre türevidir.

$g(x) = 1+x+x^2+x^3+\ldots =1/(1-x) =(1-x)^{-1}$ dir. g(x) $a_r =1$ için üretken fonksiyondur.
$h(x)= (g(x))^n= (1/(1-x))^n=(1-x)^{-n}$ dir. h(x), $a_r =C(r+n-1,r)$ için üretken fonksiyondur.

Örnek: $a_r=3r+5r^2$ için üretken fonksiyonu bulunuz.

Çözüm: g(x)=1/(1-x) olsun. 1 için üretken fonksiyon g(x) dir. Böylece r için üretken fonksiyon xg'(x) dir. teoremin e şıkkını tekrar uygulayarak r^2 için üretken fonksiyon x(xg'(x))' bulunur.

Böylece aranan üretken fonksiyon 3.xg’(x)+5. x(xg’(x))’ = $\frac{3x}{(1-x)^2}+\frac{5x+5x^2}{(1-x)^3}$ bulunur

3.2 Üstel Üretken Fonksiyonlar.

Sıradan üretken fonksiyonlar, benzer nesnelerin farklı konumlara(sıra önemli değil) dağıtım problemlerini çözmek için kullanılır. Şimdi düzenleme probleminde sıranın önemli olduğu problemler göz önüne alınacaktır. Örnek olarak, beş kırmızı bilyanın üç farklı kutuya koyulabilme şekillerinde sıra önemli değildir. Oysa, üç farklı renkteki(kırmızı, mavi ve beyaz) bilyanın 5 tanesinin bir satıra koyulması probleminde sıra önemli bir rol oynar. Her ne kadar KKMMB(Kırmızı,Kırmızı,Mavi;Mavi,Beyaz) ile KMKMB ((Kırmızı, Mavi;Kırmızı, Mavi, Beyaz) düzenlemesinde aynı sayıdaki renk bilya olsa da bunlar aynı düzenleme değildir. Bu şekilde sıranın önemli olduğu kombinasyonel problemlerin çözümündeki üretken fonksiyonlara üstel(exponential) üretken fonksiyonlar denir. Bunu bir örnek ile açıklayalım.

Örnek: Üç renkli(kırmızı,mavi ve beyaz) bilyalardan 5 tanesini bir satırda her renkten en az bir tane olacak şekilde kaç türlü düzenleyebiliriz?

Çözüm: Bilyaların sayıları toplamı her biri en az 1 olacak şekilde, kırmızı(k),mavi(m), beyaz(b), k+m+b=5 olur. Böyle bir dizilişin sayısı önceki bilgilerimizden k,m,b nin kısmi seçilmesi olup, 5!/(k!)(m!)(b!) olacaktır. Böylece toplam düzenlemenin sayısı (k+m+b)!/(k!)(m!)(b!) olup k+m+b=5 olacak ve her bir değişken en az bir değerini alacaktır. Seçimler aşağıdaki gibi olur.

k	m	b
3	1	1
1	3	1
1	1	3
2	2	1
2	1	2
1	2	2

Böylece düzenlemenin toplam sayısı;

$$\frac{5!}{(3!)(1!)(1!)}+\frac{5!}{(1!)(3!)(1!)}+\frac{5!}{(1!)(1!)(3!)}+\frac{5!}{(2!)(2!)(1!)}+\frac{5!}{(2!)(1!)(2!)}+\frac{5!}{(1!)(2!)(2!)}=150$$

Şimdi $g(x)=(x/(1!)+x^2/(2!)+x^3/(3!))^3$ fonksiyonunda $x^5/(5!)$’in katsayısı önceki paragrafta toplam düzenleme sayısını veren altı ifadenin toplamıdır. g(x) fonksiyonu, üstel üretken fonksiyonun örneğidir. Sıradan üretken fonksiyonlarda olduğu gibi, polinomun 3.kuvvetini ve tek renk bilya düzenlemede 1,2 veya 3 kere gözüktüğü için polinomdaki değişkenlerin 1,2 ve 3 kuvvetlerini alırız. Burada basit üretken fonksiyonlardan önemli bir fark, polinomdaki x^r nin katsayısının $x^r/(r!)$ olması ve kombinasyonel problemin çözümü, üstel üretken fonksiyonda $x^r/(r!)$ nin katsayısıdır. Şimdi g(x)’te $x^5/(5!)$’in katsayısını bulmak için daha kolay bir yol varmıdır? $h(x)=(e^x-1)^3$ olsun, burada x herhangi bir değişken olmak üzere, e^x, $1+x+x^2/(2!)+x^3/(3!)+\ldots$ ile tanımlanan üstel fonksiyon(kuvvet serisi) dir. Buradan gerekli katsayı, $h(x) = (e^{3x}-3e^{2x}+3e^x-1)$ deki $x^5/(5!)$’in katsayısıdır ve bu katsayı $3^5-(3)2^5+3=150$’dir.

Tanım:
Eğer, $b_r(r=0,1,2,\ldots.)$ kombinasyonel fonksiyonun çözümü ise, $b_0+b_1x+b_2x^2/(2!) +b_3x^3)/(3!)+\ldots.$ ile tanımlanan g(x) bu problem için üstel üretken fonksiyon olarak tanımlanır.

Örnek: n elemanlı bir kümeden r farklı elemanın düzenleme sayısı b_r için üstel üretken fonksiyonu bulunuz.

Çözüm: Elbette b_r=P(n,r) dir, böylece bu problem için üretken fonksiyon, (x^r)nin katsayıları =[P(n,r)]/(r!)=C(n,r) olan bir g(x) kuvvet serisidir. Böylece, P(n,r) için üstel üretken fonksiyon, C(n,r) basit üretken fonksiyonu ile aynı olan $(1+x)^n$ dir.

Teorem:
k çeşit nesne olduğu kabul edilsin.

(a) Bu tür nesneler için limitsiz kaynak var ise, bu k tür nesnenin r(r=1,2,..) permutasyonunun sayısı, g(x) üstel üretken fonksiyondaki $x^r/r!$ nin katsayısıdır.

$$g(x)=(1+x+x^2/2!+x^3/3!+\ldots)^k=e^{kx}$$

(b) Eğer i tipindeki nesne en fazla n_i ise(i=1,2,,k) r-permutasyonun sayısı;
$h(x)=(1+x+x^2/2!+\ldots+x^{n1}/n_1!)(1+x+x^2/2!+\ldots+x^{n2}/n_2!)\ldots\ldots\ldots(1+x+x^2/2!+\ldots+x^{nk}/n_k!)$'deki $x^r/r!$ nin katsayısı olacaktır.

(c) (n!).S(r,n)= $(e^x-1)^n$ deki $x^r/r!$ nin katsayısıdır.

Örnek: I,M,S ve P harfleri ile oluşturulan r-permutasyonun sayısını bulun. Burada, r pozitif bir tamsayıdır.
Çözüm: r-permutasyonun sayısı, $g(x)=e^{4x}$ üstel üretken fonksiyonunda $x^r/r!$ Teriminin katsayısı olacaktır. Bu ise, 4^r dir.

Örnek: 9 kişi, 4 odaya, tamamı bir odada olmayacak şekilde kaç türlü yerleştirilebilir?

Çözüm: Eğer x, bir odaya yerleştirilen kişi sayısı olursa, x en az bir en fazla 6 olmalı ve 4 oda vardır. Böylece bu kombinasyonel problem için üstel üretken fonksiyon;

$g(x)=(x+x^2/2!+x^3/3!+\ldots+x^6/6!)^4$ dir. Şimdi, 9 kişinin 4 odaya yerleştirilme yollarının sayısı g(x)'deki $x^9/9!$ teriminin katsayısıdır ve bu katsayı,

$$h(x)=(e^x-1)^4=(e^4x-4e^{3x}+6e^{2x}-4e^x+1)^4 \text{ deki } x^9/9! \text{ in katsayısıdır.}$$

Böylece, düzenlemenin sayısı, $4^9-(4)3^9+(6)2^9-4$ olacaktır.(Düzenlemenin sayısının (4!)S(9,4) olduğuna dikkat edin. Burada S(9,4) daha önce açıklanan ikinci tür stirling sayısıdır.